إطار الأمن السيبراني للمصارف والمؤسسات المالية

CYBERSECURITY FRAMEWORK FOR BANKS AND FINANCIAL INSTITUTIONS

يناير 2026م

تمهيد

يشهد النظام المالي العالمي تحولاً تقنياً متسارعاً أحدث تغييراً عميقاً في كيفية تقديم الخدمات المالية واستخدامها. ومع توسع الرقمنة وتزايد مستويات الترابط داخل القطاع المصرفي والمالي وبين مزوّدي الخدمات الخارجيين، تنمو مخاطر الأمن السيبراني في حجمها وتعقيدها وتأثيرها، مما يجعلها أحد أبرز التحديات التي تواجه المؤسسات المصرفية والمالية، بل وتمس استقرار القطاع المالي ومرونته على المستوى الكلي.

إدراكاً لهذه التحديات المتصاعدة، يضع بنك السودان المركزي قضايا الأمن السيبراني والمرونة السيبرانية في صدارة أولوياته التنظيمية والرقابية. نسبة لازياد اعتماد القطاع المصرفي والمالي السوداني على الخدمات المالية الرقمية، واستخدام مزوّدي الخدمات التقنية من الأطراف الثالثة، وهي تطورات على الرغم من أثرها الإيجابي في تعزيز الكفاءة والشمول المالي، إلا أنها تزيد من تعرض القطاع للتهديدات والهجمات السيبرانية. وانطلاقاً من دوره الرقابي، يتخذ بنك السودان المركزي هذه الخطوة الاستباقية الرامية إلى رفع قدرة القطاع على تخفيف المخاطر السيبرانية، واكتشافها، والاستجابة لها، والتعافي منها بكفاءة.

في هذا السياق، يُصدر بنك السودان المركزي إطار الأمن السيبراني للقطاع المصرفي والمالي بوصفه مرجعاً تنظيمياً شاملاً يهدف إلى دعم الجهات الخاضعة لرقابته في ترسيخ حوكمة فعّالة للأمن السيبراني، وتطبيق ضوابط فنية وتشغيلية قوية، ورفع مستويات النضج والجاهزية، وبناء منظومة قادرة على الصمود أمام التهديدات والاضطرابات السيبرانية. حيث تم تطوير هذا الإطار استناداً إلى أبرز المعايير والممارسات الدولية، بما يتوافق مع خصوصية البيئة المصرفية والمالية في السودان، بما يضمن سهولة تطبيقه ووضوح متطلباته.

يؤكد بنك السودان المركزي أن نجاح تطبيق هذا الإطار يستلزم التزاماً كاملاً من مجالس الإدارات والإدارة التنفيذية في جميع المصارف والمؤسسات المالية، إلى جانب تعزيز التعاون وتبادل المعلومات داخل القطاع. إن بناء بيئة مصرفية رقمية آمنة لا يتحقق بالضوابط وحدها، بل يقوم على رؤية مشتركة، وتطوير مستمر للقدرات، وشعور متجدد بالمسؤولية الجماعية.

يجدد بنك السودان المركزي التزامه بتوفير الدعم والإشراف اللازمين لتعزيز أمن ومرونة القطاع المصرفي والمالي، وضمان حماية أصوله الرقمية، والمحافظة على الاستقرار المالي، ودعم مسيرة التنمية الإقتصادية في البلاد.

آمنة ميرغني حسن التوم

المحافظ

بنك السودان المركزي

المحتويات

قائمة المصطلحات Glossary

CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System.
CWE/SANS	Common Weakness Enumeration/ SysAdmin, Audit, Network and Security
DDOS	Distributed Denial-of-Service (DDoS) attack
ECC	Error Code Correction RAM
ISO27001	Information security standard
GPS	Global Positioning System
NIST	National Institute of Standards and Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion prevention system
MITER ATT& CK	Adversarial Tactics, Techniques, and Common Knowledge
OWASP	Open Web Application Security Project
RPC	Remote Procedure Call
SIEM	Security Information and Event Management
S/MIME	(Secure/Multipurpose Internet Mail Extensions)
TTPS	Trusted Transport Protocol Suite

1. المقدمة

في ظل التطور التكنولوجي والتحول الرقمي المتسارع الذي تشهده الصناعة المصرفية والمالية، أصبحت الهجمات السيبرانية تشكل تهديداً خطيراً للنظام المالي بأكمله، إذ تتزايد طبيعتها وتعقيدها بفعل عدة عوامل، من أبرزها التطور التقني المستمر، والترابط المتنامي بين المؤسسات المالية والأطراف الخارجية، إلى جانب الجهود المستمرة التي يبذلها قراصنة الإنترنت لاكتشاف أساليب جديدة لاختراق أنظمة تكنولوجيا المعلومات والإتصالات، مستغلين جاذبية تلك المؤسسات كمصدر لتحقيق مكاسب مالية غير مشروعة.

في هذا السياق، اتخذت السلطات التنظيمية والرقابية في مختلف دول العالم تدابير تهدف إلى تمكين المؤسسات المالية من تخفيف المخاطر السيبرانية، وتعزيز قدرتها على الإستجابة الفعالة للهجمات السيبرانية والتعافي منها.

انطلاقاً من هذا التوجه، بذل بنك السودان المركزي جهوداً حثيثة لتصميم وإصدار إطار الأمن السيبراني، بهدف تمكين جميع الجهات الخاضعة لرقابته وإشرافه من تحديد المخاطر السيبرانية، إدارتها بفعالية، ضمان حماية أصول المعلومات والخدمات الإلكترونية ، وتعزيز المرونة والصمود السيبراني في القطاع المصرفي والمالي السوداني.

يستند هذا الإطار إلى القوانين المنظمة للعمل المصرفي والمالي في جمهورية السودان، متطلبات بنك السودان المركزي، معايير الأمن السيبراني مثل NIST، ISF، ISO، BASEL، وPCI-DSS، بالإضافة إلى أفضل الممارسات الدولية المتبعة لدى البنوك المركزية في هذا المجال.

يشتمل الإطار على أهم المصطلحات والتعريفات الخاصة بالأمن السيبراني، نطاق ومسؤولية التطبيق، والإطار المفاهيمي الذي يشتمل على الأهداف والمنهجية المتبعة لإعداده، إضافة إلى مبادئ تنفيذ الأمن السيبراني الفعال، ومستوى النضج المستهدف. كما يتضمن الإطار تسعة أقسام رئيسية هي:

(1) الحوكمة والقيادة.

(2) إدارة المخاطر السيبرانية.

(3) الضوابط الفنية والتشغيلية.

(4) الأمن السيبراني للخدمات المالية الإلكترونية.

(5) إدارة الأزمات والتخطيط للطوارئ.

(6) الأمن السيبراني للطرف الثالث.

(7) الإلتزام والمراجعة.

(8) التعاون.

(9) التقييم.

2. التعريفات

تكون للعبارات والكلمات التالية الواردة بالإطار المعاني الموضحة أمام كل منها، ما لم يقتض السياق معنى آخر:

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.1 سيبراني (Cyber)	يتعلق بالبنية التحتية المعلوماتية المترابطة، أو مايتم ضمنها أو خلالها من تفاعلات بين الأشخاص والعمليات والبيانات وأنظمة المعلومات.	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems
2.2 تنبيه سيبراني (Cyber Alert)	إشعار بوقوع حادثه سيبراني محدد، أو بوجود تهديد سيبراني موجه إلى إلى أنظمة المعلومات الخاصة بالمؤسسة.	Notification that a specific cyber incident has occurred, or a cyber threat has been directed at an organisation's information systems.
2.3 هجوم سيبران (Cyber Attack)	محاولة أو محاولات خبيثة لاستغلال الثغرات الأمنية من عبر الوسائط السيبرانية بهدف إتلاف الأصول أو تعطيلها أو الوصول غير المصرح إليها.	Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.
2.4 حدث سيبراني (Cyber Event)	أي حدث يمكن ملاحظته في نظام معلومات، وقد تشير بعض الأحداث السيبرانية إلى أن حادثاً سيبرانياً قيد الحدوث.	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
2.5 حادث سيبراني (Cyber Incident)	حدث سيبراني يؤثر سلباً على الأمن السيبراني لنظام معلومات، أو على المعلومات التي يعالجها أو يخزنها أو ينقلها، سواء كان ناتجاً عن نشاط خبيث أم غير خبيث.	A cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not.
2.6 خطة الاستجابة للحوادث السيبرانية (Cyber Incident Response Plan)	توثيق لمجموعة من التعليمات أو الإجراءات المحددة مسبقاً، تهدف إلى الاستجابة للحوادث السيبرانية والحد من آثارها.	The documentation of a predetermined set of instructions or procedures to guide the response to, and limit consequences of a cyber incident
2.7 المرونة السيبرانية (Cyber Resilience)	قدرة المؤسسة على مواصلة أداء مهمتها من خلال التنبؤ بالتهديدات السيبرانية والتغيرات الأخرى ذات الصلة في البيئة والتكيف معها، بالإضافة إلى الصمود أمام الحوادث السيبرانية واحتوائها والتعافي منها بسرعة.	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.8 المخاطر السيبرانية (Cyber Risk)	مزيج من احتمالية وقوع الحوادث السيبرانية وحجم تأثيرها.	The combination of the probability of cyber incidents occurring and their impact.
2.9 الأمن السيبراني (Cyber Security)	مجموعة من الأدوات، السياسات، المفاهيم الأمنية، الضمانات، الإرشادات، منهجيات إدارة المخاطر، الإجراءات، التدريب، أفضل الممارسات، التقنيات، والتدابير الكفيلة بحماية أصول المعلومات لدى الجهة من التهديدات الداخلية والخارجية.	A collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the organization's information assets against internal and external threats.
2.10 تهديد سيبراني (Cyber Threat)	حالة تنطوي على إمكانية استغلال ثغرة أمنية واحدة أو أكثر، وقد تؤثر سلباً على الأمن السيبراني.	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.
2.11 خرق البيانات (Data Breach)	إختراق أمني يؤدي إلى التدمير العرضي أو غير القانوني، أو الفقدان، أو التغيير، أو الكشف غير المصرح به إلى البيانات التي يتم نقلها، أو تخزينها، أو معالجتها بأي بطريقة أخرى.	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.
2.12 الأمن الدفاعي المتعمق (Defence-in-Depth)	استراتيجية تدمج الأفراد والعمليات والتقنيات لإنشاء مجموعة متنوعة من الحواجز عبر طبقات أو أبعاد متعددة داخل المؤسسة.	Strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.
2.13 رفض الخدمة (Denial of Service) (DoS	منع الوصول المصرح به إلى المعلومات أو أنظمة المعلومات، أو تأخير عمليات ووظائف أنظمة المعلومات، مما يؤدي إلى فقدان إمكانية الوصول إليها من قبل المستخدمين المصرح لهم.	Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users.
2.14 رفض الخدمة الموزع (Distributed Denial) (of Service DDoS	محاولة خبيثة لتعطيل حركة مرور الحزم العادية لمخدم أو خدمة أو شبكة مستهدفة من خلال إغراقها بفيض من الحزم من مصادر متعددة. بهدف جعل الخدمة غير متاحة لمستخدميها المستهدفين.	A malicious attempt to disrupt the normal traffic of a targeted service, server, or network by overwhelming it with a massive flood of packets from multiple sources, thereby preventing legitimate users from accessing the service.
2.15 البرمجيات الخبيثة (Malware)	برامج تصمم بقصد خبيث، وتحتوي على خصائص أو قدرات قد تسبب ضرراً مباشراً أو غير مباشر للمؤسسات أو أنظمة المعلومات الخاصة بها.	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.16 التصيد الاحتيالي (Phishing)	شكل رقمي من أشكال الهندسة الاجتماعية يهدف إلى الحصول على معلومات خاصة أو سرية من خلال انتحال صفة كيان موثوق به في تواصل إلكتروني.	A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.
2.17 برامج الفدية (Ransomware)	برمجيات خبيثة تُستخدم في الابتزاز من خلال تعطيل استخدام نظام المعلومات أو البيانات المرتبطة به، إلى حين الاستجابة لمطلب الفدية.	Malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied.
2.18 مسؤول المخاطر (Risk Owner)	الشخص او الجهة التي تتحمل المسؤولية الكاملة عن متابعة خطر معين و لديه/ لديها السلطة لاتخاذ الاجراءات المناسبة لإدارته.	A person or entity with the accountability and authority to manage a risk
2.19 الإستجابة (Risk Response)	قرار وإجراءات مقصودة ومبنية على معرفة مسبقة تهدف الى قبول او تجنب أو تخفيف أو مشاركة أو نقل الخطر المحدد.	Intentional and informed decision and action to accept, avoid, mitigate, share or transfer an identified risk.
2.20 تحديد الأصول (Asset Identification)	عملية تتم لتحديد الأصول المملوكة أو التي تديرها الجهة المرخصة بشكل فريد، بناء علي معطيات معروفة عن الأصول.	The process carried out to uniquely identify the assets owned or managed by the licensed entity, based on known and defined information about those assets.
2.21 السبب الجذري (Root Cause)	السبب الأساسي وراء حادث أمني أو ثغرة، مثل خرق البيانات أو هجوم البرمجيات الخبيثة. يُعتبر تحديد السبب الجذري أمرًا ضروريًا لحل المشكلات بشكل فعال ومنع حدوثها في المستقبل.	the fundamental reason behind a security incident or vulnerability, such as a data breach or malware attack. Identifying the root cause is essential for effectively resolving issues and preventing future occurrences.
2.22 النسخ الاحتيالي (Skimming)	عملية احتيالية يتم فيها نسخ البيانات المخزنة على الشريط الممغنط لبطاقات الدفع باستخدام أجهزة غير مشروعة، غالبا عند أجهزة الصراف الآلي أو نقاط البيع، بغرض استخدامها في تزوير البطاقات أو تنفيذ معاملات غير مصرّح بها.	A fraudulent process in which the data stored on the magnetic stripe of payment cards is copied using illicit devices, often at ATMs or point-of-sale terminals, with the intent of using it to clone cards or carry out unauthorized transactions.
2.23 خصائص الأمان المادية (Physical Security Features)	خصائص الأمان المادية للمستندات هي السمات والعلامات المدمجة في المستندات الرسمية (مثل العلامات المائية، الأحبار الخاصة، الطباعة الدقيقة، الشرائط الأمنية، أو الهولوجرام) والتي تهدف إلى التحقق من أصالة المستند ومنع تزويره أو تعديله.	The physical security features of documents are the characteristics and embedded markers in official documents (such as watermarks, special inks, microprinting, security threads, or holograms) designed to verify the authenticity of the document and prevent its forgery or alteration.

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.24 شهية المخاطرة (Risk appetite)	مقدار ونوع المخاطر التي ترغب الجهة في قبولها في سعيها لتحقيق أهدافها.	The amount and type of risk that an organization is willing to accept in pursuit of its objectives.
2.25 الحوسبة السحابية (Cloud computing)	تقديم خدمات الحوسبة عبر الإنترنت، مع نماذج خدمة متنوعة مثل البنية التحتية كخدمة (IaaS) ، والبيئة كخدمة (PaaS) ، والبرمجيات كخدمة.(SaaS)	The delivery of computing services over the internet, With various service models—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
2.26 نمذجة التهديدات (Threat Modelling)	ممارسة استباقية في الأمن السيبراني تتضمن تحديد وتقييم وترتيب التهديدات المحتملة لنظام أو تطبيق. يحلل هذه العملية بنية وتصميم النظام لكشف الثغرات وفهم كيفية استغلال التهديدات المختلفة لها. توفر الأطر الشائعة المستخدمة في نمذجة التهديدات، مثل (OCTAVE, STRIDE, PASTA) ، منهجيات منظمة لتقييم التهديدات.	A proactive cybersecurity practice that involves identifying, assessing, and prioritizing potential threats to a system or application. This process analyses the architecture and design of the system to uncover vulnerabilities and understand how various threats might exploit them. Common frameworks used in threat modelling, such as STRIDE, PASTA, and OCTAVE, provide systematic methodologies for evaluating threats.
2.27 الذكاء الإصطناعي (Artificial Intelligence)	محاكاة عمليات الذكاء البشري بواسطة الآلات، خاصةً أنظمة الكمبيوتر. تشمل مجموعة من التقنيات، بما في ذلك التعلم الآلي، ومعالجة اللغة الطبيعية، ورؤية الكمبيوتر، مما يمكّن الآلات من أداء مهام تتطلب عادةً الذكاء البشري، مثل فهم اللغة، والتعرف على الأنماط، واتخاذ القرارات.	Simulation of human intelligence processes by machines, particularly computer systems. It encompasses a range of technologies, including machine learning, natural language processing, and computer vision, enabling machines to perform tasks that typically require human intelligence, such as understanding language, recognizing patterns, and making decisions.
2.28 الكود المصدري (Source Code)	مجموعة من التعليمات والبيانات القابلة للقراءة البشرية المكتوبة بلغة برمجة، والتي تحدد كيفية عمل تطبيقات البرمجيات. يُعتبر الكود المصدري أساسيًا للتعاون بين المطورين، حيث يمكن مشاركته والتحكم في نسخه ومراجعته لضمان الجودة والوظائف.	Is the human-readable set of instructions and statements written in a programming language that defines how software applications operate. Source code is essential for collaboration among developers, as it can be shared, version-controlled, and reviewed to ensure quality and functionality.
2.29 الأتمتة (Automation)	استخدام التكنولوجيا لأداء المهام مع الحد الأدنى من التدخل البشري، مما يسهل العمليات لتحسين الكفاءة والدقة والسرعة. مع استمرار تقدم الأتمتة، لديها القدرة على تحويل الصناعات، وزيادة الإنتاجية، ودفع	Use of technology to perform tasks with minimal human intervention, streamlining processes to improve efficiency, accuracy, and speed. As automation continues to advance, it has the potential to transform industries, enhance

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
	الابتكار، بينما تثير أيضًا اعتبارات حول استبدال القوة العاملة والحاجة إلى مهارات جديدة.	productivity, and drive innovation, while also raising considerations around workforce displacement and the need for new skills.
2.30 تعلم الآلة (Machine learning)	فرع من فروع الذكاء الاصطناعي يمكّن الأنظمة من التعلم من البيانات وتحسين أدائها بمرور الوقت دون برمجة واضحة. يتضمن ذلك خوارزميات تحلل الأنماط وتقوم بعمل توقعات أو قرارات استنادًا إلى البيانات المدخلة.	A subset of artificial intelligence that enables systems to learn from data and improve their performance over time without explicit programming. It involves algorithms that analyse patterns and make predictions or decisions based on input data.
2.31 الثقة الصفرية (Zero trust)	نموذج أمني يعمل على مبدأ "لا تثق أبدًا، تحقق دائمًا"، حيث يتطلب التحقق الصارم من هوية كل مستخدم وجهاز يحاول الوصول إلى الموارد، بغض النظر عن موقعه. يقلل هذا النهج من خطر خروقات البيانات من خلال افتراض أن التهديدات قد تنشأ من خارج الشبكة وداخلها.	A security model that operates on the principle of "never trust, always verify," requiring strict identity verification for every user and device attempting to access resources, regardless of their location. This approach minimizes the risk of data breaches by assuming that threats could originate from both outside and inside the network.
2.32 سلسلة الكتل (Blockchain)	تقنية دفتر أستاذ رقمي لامركزي وموزع تسجل المعاملات بشكل آمن عبر عدة أجهزة كمبيوتر، مما يضمن عدم إمكانية تعديل البيانات بأثر رجعي. تجعل هذه الشفافية والثبات منها تقنية أساسية للعملات الرقمية، والعقود الذكية، ومجموعة متنوعة من التطبيقات في مجالات مثل التمويل وسلسلة الأمداد والرعاية الصحية.	A decentralized and distributed digital ledger technology that securely records transactions across multiple computers, ensuring that the data cannot be altered retroactively. This transparency and immutability make it a foundational technology for cryptocurrencies, smart contracts, and various applications across industries like finance, supply chain, and healthcare.
2.33 الحاجة الى الإمتلاك (The need to possess)	الحوجة إلى التملك أو السيطرة. مبدأ يبرر تمسك الجهة بالسرية والنزاهة، ويضمن أن تظل حيازتها لأصولها الرقمية الخاصة آمنة وموثوقة وغير قابلة للطعن.	A principle that justifies an entity's commitment to confidentiality and integrity, ensuring that its ownership of digital assets remains secure, trustworthy, and indisputable.
2.34 الحاجة الي المعرفة (The Need to know)	مفهوم أمن المعلومات الذي يقيد الوصول إلى البيانات بما هو ضروري فقط لتمكين المستخدم من أداء وظيفته.	The concept of information security that restricts access to data to only what is necessary for the user to perform their job.
2.35 الموظفين الخارجيين (External Personnel)	موظفوا الجهة الذين يدخلون إلى أنظمة الجهة من مصادر خارجية (مثل أجهزة الكمبيوتر المحمولة الخاصة بهم).	Employees' access to the organization's systems remotely from non-affiliated sources (such as personal computers).

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.36 الحسابات المميزة غيرالشخصية (Non-Personal Premium Accounts)	حسابات نظام غير مرتبطة بمستخدم بشري محدد، ولكنها تتمتع بصلاحيات إدارية. تُستخدم هذه الحسابات غالبًا من قِبل التطبيقات أو الخدمات أو العمليات الآلية لأداء وظائف محددة، وغالبًا ما تكون مشتركة.	System accounts not linked to a specific human user but have administrative privileges. These accounts are often used by applications, services, or automated processes to perform specific functions and are frequently shared.
2.37 مصادقة التحدي والإستجابة (Challenge-response Authentication)	بروتوكول أمان، حيث يقدم أحد الطرفين، وهو المُتحقق (عادةً المخدم)، سؤالاً فريداً، أو تحدياً، إلى طرف آخر، وهو المُطالب (عادةً مستخدم أو جهاز)، والذي يجب عليه تقديم رد صحيح لتتم مصادقته.	A security protocol in which one party, the verifier (usually the server), presents a unique question or challenge to another party, the claimant (typically a user or device), which must provide the correct response to be authenticated.
2.38 آليات مصادقة مشفرة قائمة على النماذج (Form-based cryptographic authentication mechanisms)	المصادقة التشفيرية القائمة على النماذج هي أفضل ممارسات الأمان التي تحمي كلمات مرور المستخدمين أثناء الإرسال بتحويلها إلى رموز على جهاز العميل قبل إرسالها. وهي إجراء دفاعي شامل تفرضه معايير الأمن السيبراني الحديثة للعمل بالتزامن مع وسائل حماية أخرى مثل HTTPS.	Cryptographic model-based authentication is a security best practice that protects user passwords during transmission by hashing them on the client device before sending. It is a comprehensive defensive measure mandated by modern cybersecurity standards to work in conjunction with other protective means, such as HTTPS.
2.39 جدار الحماية (Firewall Appliance)	هو جهاز مخصص من الأجهزة المصممة للمراقبة والتحكم في حركة مرور الشبكة الواردة والصادرة بناءً على قواعد أمان محددة مسبقاً. يعمل كحاجز بين شبكة داخلية موثوقة والشبكات الخارجية غير الموثوقة، مثل الإنترنت. من خلال فحص حزم البيانات، يمكن لجدار الحماية منع الوصول غير المصرح به، ومنع التهديدات السيبرانية، وتطبيق سياسات الأمان.	Is a dedicated hardware device designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. By inspecting data packets, the firewall can block unauthorized access, prevent cyber threats, and enforce security policies.
2.40 جدار حماية طبقة التطبيقات (Application Layer Firewall)	حل أمني مصمم خصيصاً لحماية تطبيقات الويب من خلال تنقية ومراقبة حركة مرور حزم الشبكة العنكبوتية بين التطبيق والإنترنت. يعمل الجدار على مستوى طبقة التطبيق، حيث يحلل الطلبات والاستجابات لتحديد ومنع الأنشطة الضارة مثل الحقن الضار، والبرمجة النصية غير المشروعة عبر المواقع، وغيرها من الثغرات.	A security solution specifically designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. A WAF operates at the application layer, analysing requests and responses to identify and block malicious activities such as SQL injection, cross-site scripting (XSS), and other vulnerabilities.

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
2.41 قواعد البيانات (Databases)	أصل يحتوي على معلومات المؤسسة الأكثر حساسيةً وخضوعًا للحماية. الهدف الأساسي هو حماية سرية بياناتها وسلامتها وتوافرها	An asset that contains the organization's most sensitive and protected information. The primary goal is to safeguard the confidentiality, integrity, and availability of its data.
2.42 القائمة البيضاء (Whitelist)	أداة تحكم قوية وموصى بها من قِبل المعايير، حيث تفرض وضع "الرفض الافتراضي"، مما يسمح بتشغيل البرامج المصرح لها فقط، مما يوفر حماية قوية ضد البرامج الضارة المعروفة وغير المعروفة.	A powerful control tool recommended by standards, enforcing a "default deny" stance that allows only authorized programs to run. This provides strong protection against both known and unknown malware.
2.43 القائمة السوداء (Blacklist)	إنشاء قائمة بالتطبيقات الضارة أو غير المرغوب فيها، ثم حظر تشغيلها على جهاز كمبيوتر أو شبكة.	Creating a list of harmful or unwanted applications and subsequently blocking their execution on a computer or network.
2.44 مجاميع التحقق (checksums)	سلسلة قصيرة ثابتة الحجم من الأحرف والأرقام، الهدف الأساسي من اختبارها في مجال الأمن السيبراني هو التحقق من سلامة البيانات. فهو يجيب على السؤال الحاسم: "هل تعرّضت هذه البيانات للتغيير أو التلف أثناء النقل أو التخزين؟"	A checksum is a fixed-size string of characters and numbers, and its primary purpose in cybersecurity is to verify data integrity. It answers the crucial question: "Has this data been altered or corrupted during transmission or storage?"
2.45 المصادقة (Authentication)	عملية التحقق من هوية المستخدم أو الجهاز أو النظام. تُعرّف معايير الأمن السيبراني المصادقة بناءً على ثلاثة أنواع رئيسية من الأدلة، أو "العوامل"، التي يُمكن تقديمها: 1. شيء تعرفه : هذا هو العامل الأكثر شيوعًا. إنه معلومة سرية لا ينبغي لأحد سواك معرفتها. (كلمة مرور، أو رقم تعريف شخصي (PIN)) 2. شيء تملكه : هذا هو شيء مادي أو رمز مميز بحوزتك. (بطاقة ذكية، أو مفتاح امان) 3. شيء أنت : هذه سمة بيولوجية - بياناتك البيومترية (البصمة).	The process of verifying the identity of a user, device, or system. Cybersecurity standards define authentication based on three main types of evidence, or "factors," that can be presented: 1. Something You Know: This is the most common factor, consisting of a secret piece of information that only you should know (e.g., a password or PIN). 2. Something You Have: This refers to a physical item or token in your possession (e.g., a smart card or security key). 3. Something You Are: This is a biological characteristic—your biometric data (e.g., fingerprint).
2.46 التوقيع الرقمي	نظام رياضي يُستخدم للتحقق من صحة وسلامة الرسالة أو المستند الرقمي. وهو في الأساس "بصمة"	A digital signature is a mathematical system used to verify the authenticity and integrity of a message or digital document. Essentially, it is an

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
(Digital signature)[1]	إلكترونية مشفرة تُثبت عدم تعديل المستند بعد توقيعه، وتُثبت هوية المُوقّع. عدم الإنكار: يُلزم المُوقّع قانونيًا بالوثيقة. لا يُمكن للمُوقّع لاحقًا إنكار توقيعه عليها، لأن التوقيع مرتبط ارتباطًا وثيقًا بمفتاحه الخاص (الذي يتحمل مسؤولية حمايته). تعتمد عملية التوقيع الرقمي على البنية التحتية للمفتاح العام (PKI) والتشفير غير المتماثل، والذي يستخدم مفتاحين مرتبطين رياضيًا: مفتاح عام ومفتاح خاص.	encrypted "fingerprint" that proves the document has not been altered after signing and establishes the identity of the signer. Non-repudiation: This legally binds the signer to the document, preventing them from later denying their signature, as it is closely linked to their private key (which they are responsible for protecting). The process of digital signing relies on a Public Key Infrastructure (PKI) and asymmetric encryption, which utilizes two mathematically related keys: a public key and a private key.
2.47 المفتاح العام (Public key)	نصف زوج من المفاتيح التشفيرية المستخدمة في التشفير بالمفتاح العام (أو التشفير غير المتماثل). بخلاف التشفير "المتماثل" التقليدي الذي يستخدم مفتاحًا سريًا واحدًا، يستخدم التشفير غير المتماثل مفتاحين مرتبطين رياضيًا: المفتاح العام: صُمم هذا المفتاح ليُشاركه الجميع، وهو ليس سرًا، والمفتاح الخاص.	A public key is one half of a pair of cryptographic keys used in public key encryption (or asymmetric encryption). Unlike traditional "symmetric" encryption, which uses a single secret key, asymmetric encryption employs two mathematically linked keys: 1. Public Key: This key is designed to be shared with everyone and is not secret. It allows others to encrypt messages that only the corresponding private key can decrypt. 2. Private Key.
2.48 المفتاح الخاص (Private key)	كلمة مرور معقدة فائقة السرية، مرتبطة رياضياً بمفتاح عام. وهو العنصر الأساسي للتشفير غير المتماثل .يتم الاحتفاظ به بسرية تامة وأمان من قبل مالكه، لاستخدامه لفك التشفير وتأكيد هوية المرسل.	A complex, highly confidential password that is mathematically linked to a public key. It is the essential component of asymmetric encryption and is kept completely secret and secure by its owner, to be used for decryption and non-repudiation.
2.49 الجهة الموثوقة (Trusted Third-party)	الطرف الثالث الموثوق به هو طرفٌ أو جهة خارجية يثق به كيانٌ ما لأداء خدماتٍ مُعينةٍ له بأمانة. ، مثل هيئة المصادقة، التي يثق بها عملاؤها لأداء خدمات معينة (مثل إصدار الشهادات الرقمية و توليدَ مفاتيحِ تشفير).	Trusted third party (TTP) is an external entity that is trusted by an organization to perform certain services reliably, such as a Certificate Authority (CA), which its clients trust to carry out specific

[1] تم تعريف التوقيع الرقمي في قانون المعاملات الإلكترونية لسنة 2007 لجمهورية السودان.

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
		functions (like issuing digital certificates and generating encryption keys).
2.50 إدارة التهيئة (Configuration management)	التأكد من أن الأجهزة والبرامج والخدمات والشبكات تعمل بشكل صحيح مع إعدادات الأمان المطلوبة، وأن لا يتم تغييرها بتغييرات غير مصرح بها أو غير صحيحة. وتوثيقها وتنفيذها ومراقبتها ومراجعتها.	Ensuring that devices, software, services, and networks operate correctly with the required security settings, and that they are not altered by unauthorized or incorrect changes. This involves documenting, implementing, monitoring, and reviewing these controls.
2.51 تنظيف البيانات (Data cleansing)	عملية مستمرة لتحديد الأخطاء والتناقضات في مجموعات البيانات وتصحيحها أو إزالتها لضمان دقة المعلومات واكتمالها وتناسقها وصلاحيتها وتوقيتها	An ongoing process of identifying errors and inconsistencies in datasets and correcting or removing them to ensure the accuracy, completeness, consistency, validity, and timeliness of information.
2.52 محطة العمل (workstation)	أحد أصول المعلومات أو أحد مكونات نظام إدارة أمن المعلومات (ISMS)[2] الخاص بالجهة. تُدرج محطة العمل إلى جانب المخدمات وأجهزة الكمبيوتر المحمولة والأجهزة المحمولة كمكون نظام يتطلب فرض إعدادات محددة (على سبيل المثال، تعطيل الخدمات أو المنافذ أو البروتوكولات غير الضرورية) لتحسين وضع الأمان.	An information asset or a component of the organization's Information Security Management System (ISMS). Workstations are listed alongside servers, laptops, and mobile devices as system components that require the enforcement of specific settings (such as disabling unnecessary services, ports, or protocols) to enhance security posture.
2.53 شبكة محلية افتراضية(VLAN)	تقنية تمكين أساسية لتجزئة الشبكة. وهي عنصر تحكم أساسي لتقليل مساحة الهجوم، واحتواء الاختراقات، وتطبيق سياسات الوصول، وتدعم بشكل مباشر متطلبات أطر العمل الرئيسية مثل NIST و PCI DSS و ISO 27001.	A VLAN (Virtual Local Area Network) is a key enabling technology for network segmentation. It is a fundamental control for reducing the attack surface, containing breaches, and enforcing access policies, directly supporting the requirements of major frameworks such as NIST, PCI DSS, and ISO 27001.
2.54 التجزئة (Segmentation)	عملية تقسيم الشبكة إلى مناطق معزولة للتحكم في تدفق البيانات واحتواء أي حوادث أمنية محتملة.	The process of dividing the network into isolated zones to control the flow of data and contain any potential security incidents.
2.55 معلمات (Parameters)	المتغيرات أو الإعدادات أو الحدود القابلة للتخصيص التي تُحدد كيفية عمل عنصر التحكم الأمني أو العملية أو النظام. وهي عناصر محددة وقابلة للضبط تُترجم	The variables, settings, or customizable limits that determine how a security control, process, or system operates. They are specific and adjustable

[2] أحد مطلوبات معيار ISO27001، ISO27002

العبارة	التعريف باللغة العربية	التعريف باللغة الإنجليزية
	السياسات رفيعة المستوى والمبادئ التوجيهية المجردة إلى قواعد تقنية وتشغيلية ملموسة وقابلة للتنفيذ.	elements that translate high-level policies and abstract guidelines into concrete and actionable technical and operational rules.
2.56 البنية التحتية (Infrastructure)	الأجهزة والبرامج والشبكات والمرافق الأساسية المترابطة التي تُمكّن المؤسسة من تطوير خدمات تكنولوجيا المعلومات واختبارها وتقديمها ومراقبتها والتحكم فيها ودعمها. إنها النظام البيئي الكامل الذي تعيش فيه البيانات وتنتقل عبره.	The interconnected hardware, software, networks, and essential facilities that enable an organization to develop, test, deliver, monitor, control, and support IT services. It is the complete ecosystem in which data resides and flows.
2.57 مُشرف الأجهزة الافتراضية (Hypervisor)	المشرف الافتراضي، المعروف أيضًا باسم مراقب الآلة الافتراضية (VMM)، هو طبقة من البرمجيات أو البرامج الثابتة أو الأجهزة تُنشئ وتُشغّل الآلات الافتراضية. وهو التقنية الأساسية المُمكّنة للمحاكاة الافتراضية. موقعه المتميز يجعله "أساس الثقة" للبيئة الافتراضية بأكملها. في حال اختراق مُشرف الأجهزة الافتراضية، يُمكن للمهاجم التحكم في جميع الأجهزة الافتراضية التي تعمل عليه، متجاوزًا بذلك ضوابط الأمان الخاصة بأنظمة التشغيل.	The hypervisor, also known as the Virtual Machine Monitor (VMM), is a layer of software, firmware, or hardware that creates and runs virtual machines. It is the foundational technology that enables virtualization. Its privileged position makes it the "root of trust" for the entire virtual environment. If the hypervisor is compromised, an attacker can gain control over all virtual machines running on it.
2.58 تكتيكات وميول المهاجمين (CK & ATT)	تكتيكات وتقنيات الخصم استنادًا إلى الملاحظات الواقعية للهجمات الإلكترونية. ويمكن اعتباره بمثابة كتاب ضخم ومفصل لكيفية عمل المتسللين، ولكن تم كتابته من وجهة نظر المدافع لمساعدتهم على فهم الهجمات واكتشافها وإيقافها	The ATT&CK framework (Adversarial Tactics, Techniques, and Common Knowledge) outlines adversary tactics and techniques based on real-world observations of cyberattacks. It can be viewed as a comprehensive and detailed guide on how attackers operate, written from the defender's perspective to help them understand, detect, and mitigate attacks.

3. النطاق والمسؤولية

3.1 النطاق

يشـــمل النطاق جميع الجوانب المتعلقة بحماية الأنظمة والبيانات من التهديدات الســـيبرانية وينطبق على كافة الجهات الخاضعة لإشراف ورقابة بنك السودان المركزي.

3.2 المسؤولية

تقع مســـؤولية تطبيق إطار الأمن الســـيبراني على مجلس الإدارة، الإدارة التنفيذية ، مســـؤولي أمن المعلومات، مسـؤولي تكنولوجيا المعلومات،مسـؤولي المخاطر والإلتزام والمعنيين بتصـميم وتنفيذ ومراجعة ضـوابط وإجراءات الأمن السيبراني.

4. الإطار المفاهيمي

4.1 الأهداف

(1) إرســاء اطار مرجعي موحد لمعالجة قضــايا الأمن الســيبراني داخل الجهات الخاضــعة لإشــراف ورقابة بنك السودان المركزي ، بما يضمن اتساق السياسات والممارسات المتبعة.

(2) الوصـول إلى مسـتوى مناسـب من النضـج في ضـوابط الأمن السـيبراني، وفقاً لأفضـل الممارسـات والمعايير الدولية المعتمدة، وبما يعزز الجاهزية المؤسسية في مواجهة التهديدات السيبرانية.

(3) تعزيز المرونة السيبرانية.

(4) ضمان القدرة على مواصلة أداء المهام والوظائف، وتقديم الخدمات بشكل مستمر.

(5) تعزيز تبادل المعلومات السيبرانية على مستوى القطاع لتمكينها من اتخاذ الإجراءات الوقائية.

(6) تمكين بنك السودان المركزي من أداء دوره الإشرافي والتنظيمي على نحو فعّال.

4.2 مبادئ تنفيذ الأمن السيبر اني الفعال

(1) الحوكمة، إدارة المخاطر، والإلتزام.

(2) التعاون.

(3) تعزيز واستدامة المرونة السيبرانية.

(4) التحسين المستمر.

4.3	مستوي النضج (Maturity Level)
المبدأ	تطوير مجموعة من خطط العمل التصحيحية ذات الأولوية وتنفيذها لتحقيق مستوى النضج المستهدف، بناءً على نتائج عملية التقييم.
الهدف	استخدام برنامج أمني قوي وناضج كوسيلة للتميز وتسويق الجهة ككيان آمن وموثوق.
الضوابط	
(1)	يجب علي الجهة تقييم وقياس مستوى نضج الأمن السيبراني وفقًا لمواءمة حالة الأمن الحالية مع المجالات المشمولة في هذا الإطار. يتكون نموذج النضج من ستة مستويات، ويركز على الأفراد والسياسات والإجراءات المعمول بها، بالإضافة إلى الحلول التقنية الحالية.
(2)	ينبغي قياس مستوى نضج الأمن السيبراني باستخدام نموذج مُعدّ مسبقًا. يُميّز هذا النموذج سبعة مستويات نضج (0، 1، 2، 3، 4، 5و6)، حسب جدول مستويات النضج أدناه.
(3)	يجب على الجهة استيفاء جميع معايير مستويات النضج السابقة لتحقيق المستويات 3، 4، أو 5.
(4)	يهدف هذا الإطار إلى إرساء نهج فعال لمعالجة الأمن السيبراني وإدارة مخاطره في القطاع المالي. ولتحقيق مستوى نضج مناسب في مجال الأمن السيبراني، يجب على الجهات العمل على مستوى النضج 3 أو أعلى، كما هو موضح أدناه: أ- **مستوى النضج الثالث**: يجب على الجهة تحديد ضوابط الأمن السيبراني واعتمادها وتطبيقها. بالإضافة إلى ذلك، مراقبتها والإلتزام بوثائق الأمن السيبراني (سياسات ومعايير وإجراءات الأمن السيبراني). ب- **مستوى النضج الرابع**: يجب على الجهة قياس وتقييم فعالية ضوابط الأمن السيبراني المُطبقة بشكل دوري. ولقياس وتقييم فعالية ضوابط الأمن السيبراني، يجب تحديد مؤشرات المخاطر الرئيسية (KRIs). بحيث تُستخدم مؤشرات المخاطر الرئيسية لإعداد تقارير الإتجاهات وتحديد التحسينات المحتملة. ج- **مستوى النضج الخامس**: يجب علي الجهة تحسين ضوابط الأمن السيبراني بصورة مستمرة. ويتحقق هذا التحسين من خلال التحليل المستمر لأهداف وإنجازات الأمن السيبراني وتحديد التحسينات الهيكلية. ويجب دمج ضوابط

	الأمن السيبراني مع ممارسات إدارة المخاطر، ودعمها بمراقبة آلية آنية. بالإضافة إلى ذلك،يتم تقييم أدائها من خلال مقارنات معيارية(bench mark)مع أداء المصارف والمؤسسات المالية وبيانات القطاع. د- **مستوى النضج السادس:** هو أعلى مستوى من النضج، حيث الإستفادة من الذكاء الإصطناعي وتعلم الآلة والأتمتة والثقة الصفرية في الأمن السيبراني، وسيتم وضع ضوابط خاصة به مستقبلاً.

جدول مستويات النضج

مستوى النضج	التعريف والمعايير	الوصف
المستوى 0	▪ لا يوجد توثيق. ▪ لا يوجد وعي أو اهتمام بالأمن السيبراني.	▪ لا توجد ضوابط للأمن السيبراني. ▪ لا توجد خطط لتطبيق الأمن السيبراني. ▪ لا يوجد وعي بمخاطر ومهددات الأمن السيبراني.
المستوى 1	▪ ضوابط الأمن السيبراني مُعرَّفة جزئيًا. ▪ تُنفَّذ ضوابط الأمن السيبراني بطريقة غير منتظمة أو غير متجانسة.	▪ يختلف تصميم وتنفيذ ضوابط الأمن السيبراني باختلاف مستويات الإدارات أو الأقسام. ▪ ضوابط الأمن السيبراني لا تقلل مستوي المخاطر المُحددة إلا جزئياً.
المستوى 2	▪ يعتمد تنفيذ مراقبة الأمن السيبراني على ممارسة غير رسمية ومكتوبة، وإن كانت موحدة.	▪ توجد ضوابط للأمن السيبراني ولكن تطبق بصورة مكررة أو قابلة للتكرار. ▪ لم يتم تحديد أو اعتماد أهداف الرقابة وتصميمها رسمياً. ▪ ينظر بشكل محدود إلى المراجعة والإختبار المنظم.
المستوى 3	▪ يتم تحديد ضوابط الأمن السيبراني والموافقة عليها وتنفيذها بطريقة منظمة ورسمية. ▪ توجد خطط وتوضيحات في كيفية تطبيق ضوابط الأمن السيبراني	▪ وضع سياسات ومعايير وإجراءات الأمن السيبراني. ▪ مراقبة الإلتزام بوثائق الأمن السيبراني (السياسات والمعايير والإجراءات). ▪ يفضل استخدام أداة الحوكمة والمخاطر والإلتزام (GRC). ▪ تحديد مؤشرات الأداء الرئيسية ومراقبتها. ▪ إعداد التقارير وتقييم التنفيذ.
المستوى 4	▪ يتم تقييم فعالية ضوابط الأمن السيبراني بشكل دوري وتحسينها عند الضرورة. ▪ يتم توثيق عملية القياس والتقييم وفرص التحسين المستمر.	▪ يتم قياس فعالية ضوابط الأمن السيبراني وتقييمها دورياً. ▪ تُستخدم مؤشرات المخاطر الرئيسية وتقارير الإتجاهات لتحديد فعالية ضوابط الأمن السيبراني.

مستوى النضج	التعريف والمعايير	الوصف
		▪ تُستخدم نتائج القياس والتقييم لتحديد فرص تحسين ضوابط الأمن السيبراني.
المستوى 5	▪ تخضع ضوابط الأمن السيبراني لخطة تحسين مستمرة.	▪ يركز برنامج الأمن السيبراني على مستوى الجهة من حيث الإلتزام وفعالية، وتحسين ضوابط الأمن السيبراني. ▪ دمج ضوابط الأمن السيبراني مع إطار عمل وممارسات إدارة المخاطر. ▪ تقييم أداء ضوابط الأمن السيبراني باستخدام بيانات الجهات المماثلة والقطاعات.
المستوى 6	▪ الإستفادة من الذكاء الإصطناعي والتعلم الآلي والأتمتة والثقة الصفرية في الأمن السيبراني.	▪ اعتماد نهج استباقي وتوقعي للأمن السيبراني. ▪ استخدام تقنيات متطورة مثل الذكاء الإصطناعي/التعلم الآلي (AI/ML) للكشف عن التهديدات والإستجابة لها. ▪ إجراء محاكاة شاملة للهجمات والإختراقات السيبرانية. ▪ مشاركة دائمة ونشطة في مجال معلومات التهديدات على مستوى القطاعات. ▪ مراجعة وتحسين مستمر لجميع الضوابط الأمنية.

4.3.1	التوقعات والحد الأدنى لمستوي النضج (Expectations and Minimum (Maturity Level
المبدأ	إجراء تقييم ذاتي لنضج الجهة في كل مجال من مجالات الأمن السيبراني.
الهدف	تحقيق الإلتزام بمستوي النضج المحدد، والذي يعتبر مرحلة حيث تكون الممارسات الأمنية مستقرة ومُوثقة.
الضوابط	
(1)	يجب علي جميع الجهات السعي للوصول إلى المستوى 3 (منظمة ورسمية) كحد أدنى في معظم المجالات .
(2)	يحق لبنك السودان المركزي تحديد بعض الجهات وإلزامها بالوصول لمستويات نضج أعلى حسب ما يراه مناسباً.
(3)	يجب على الجهات (بطلب من البنك المركزي) وضع خطة لسد الفجوات ورفع مستوى نضجها، مع وجود مواعيد نهائية محددة.
(4)	إجراء تقييم ذاتي دوري (خلال فترات محددة) وتقديم التقرير إلى البنك المركزي.

5. هيكل الإطار

يتكون هيكل الإطار الموضح في الشكل أدناه من تسعة مجالات رئيسية وهي: الحوكمة والقيادة، إدارة المخاطر السيبرانية، الضوابط الفنية والتشغيلية، الأمن السيبراني للخدمات المالية الرقمية، إدارة الأزمات والتخطيط للطوارئ، الأمن السيبراني للطرف الثالث، المراجعة والإلتزام، التعاون، والتقييم.

6. الحوكمة والقيادة (Governance and Leadership)

6.1	حوكمة الأمن السيبراني (Cybersecurity Governance)
المبدأ	تحديد هيكل لحوكمة الأمن السيبراني وتنفيذه، بعد اعتماده من مجلس الإدارة.
الهدف	توجيه ومراقبة النهج العام للأمن السيبراني في الجهة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إنشاء لجنة للأمن السيبراني بموجب تفويض من مجلس الإدارة.
(2)	أن تضم اللجنة في عضويتها المناصب التالية: أ- مدراء الإدارات ذات الصلة. ب- كبير مسؤولي أمن المعلومات.
(3)	أن يترأس اللجنة أحد مديري الإدارات المعنية.
(4)	يجوز لممثل إدارة المراجعة الداخلية حضور اجتماعات اللجنة بصفة مراقب.
(5)	إعداد ميثاق للجنة الأمن السيبراني واعتماده من مجلس الإدارة، على أن يتضمن كحد أدنى مايلي: أ- أهداف اللجنة. ب- الحد الأدنى لعددالحضور في الإجتماعات. ج- دورية الإجتماعات (بحد أدنى بصورة ربع سنوية).
(6)	تعيين مدير متفرغ لوظيفة الأمن السيبراني.
(7)	أن تكون وظيفة الأمن السيبراني مستقلة عن وظيفة تقنية المعلومات، ولضمان تجنب تضارب المصالح، يجب أن يكون لكل منهما خطوط إبلاغ وميزانيات وتقييمات أداء منفصلة.
(8)	أن يقدم مسؤول الأمن السيبراني تقاريره مباشرة إلى المدير العام أو إلى مدير إحدى الإدارات الرقابية.
(9)	أن يكون كبير مسؤولي الأمن السيبراني مؤهل تأهيلاً كافياً.
(10)	الحصول على عدم ممانعة بنك السودان المركزي على تعيينه.
(11)	على مجلس الإدارة تخصيص ميزانية كافية لتنفيذ كافة أنشطة الأمن السيبراني اللازمة.

6.2	استراتيجية الأمن السيبراني (Cybersecurity Strategy)
المبدأ	تحديد استراتيجية للأمن السيبراني تكون متوائمة مع الأهداف الاستراتيجية للجهة ومع ضوابط واستراتيجية الأمن السيبراني الصادر عن بنك السودان المركزي والدولة، وأن يتم تحديثها دورياً لمواكبة التهديدات السيبرانية والتطورات التكنولوجية.
الهدف	ضمان أن تسهم مبادرات ومشروعات الأمن السيبراني داخل الجهة في تحقيق أهدافها الاستراتيجية، وأن تكون متوائمة مع استراتيجية الأمن السيبراني للقطاع المصرفي.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	وضع استراتيجية الأمن السيبراني وإعتمادها، وتحديثها بشكل دوري، وتنفيذها بفعالية.
(2)	إشراك الإدارات المعنية داخلياً والجهات الخارجية ذات الصلة في إعداد ومراجعة الاستراتيجية بشكل دوري.
(3)	أن تتوائم استراتيجية الأمن السيبراني مع ما يلي: أ- الأهداف العامة للجهة. ب- متطلبات الإلتزام القانوني والتنظيمي الخاصة بالجهة. ج- استراتيجية الأمن السيبراني للقطاع المصرفي والموجهات الصادره من بنك السودان المركزي.
(4)	أن تتناول استراتيجية الأمن السيبراني الجوانب التالية: أ- أهمية الأمن السيبراني وفوائده للجهة. ب- الحالة المستقبلية المستهدفة للأمن السيبراني، التي تمكّن الجهة من الصمود أمام التهديدات السيبرانية (الناشئة والمحتملة). ج- المبادرات والمشروعات السيبرانية التي ينبغي تنفيذها، والجدول الزمني المناسب لتحقيق الحالة المستقبلية المستهدفة. د- أن تتضمن الاستراتيجية مؤشرات أداء رئيسية (KPIs) ومؤشرات مخاطر (KRIs) لقياس مستوى التنفيذ والتحسين المستمر.

6.3	سياسة الأمن السيبراني (Cybersecurity Policy)
المبدأ	تحديد سياسة الأمن السيبراني واعتمادها وإبلاغها إلى الجهات المعنية.
الهدف	تحديد التوجهات العامة والمبادئ التنظيمية لإدارة وحماية أصول المعلومات والأنظمة و توثيق التزام الجهة وأهدافها تجاه الأمن السيبراني، وإيصال ذلك إلى أصحاب المصلحة المعنيين.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن يتم تحديد سياسة الأمن السيبراني واعتمادها من مجلس الإدارة، بحيث تغطي الجوانب الأساسية مثل حماية البيانات، التحكم في الوصول ، إدارة الحوادث ، واستمرارية الأعمال، وتعميمها علي جميع الموظفين المعنيين وتضمينها في دليل اجراءات العمل ذات العلاقة.
(2)	مراجعة سياسة الأمن السيبراني بشكل دوري وفقاً لعملية مراجعة منظمة ومحددة مسبقاً.
(3)	أ- تُؤخذ سياسة الأمن السيبراني في الإعتبار كمدخل للسياسات المؤسسية الأخرى في الجهة (مثل سياسة الموارد البشرية، والسياسة المالية، وسياسة تقنية المعلومات). ب- تكون مدعومة بمعايير وإجراءات أمنية تفصيلية (مثل معيار كلمات المرور، ومعيار جدران الحماية). ج- تستند إلى أفضل الممارسات والمعايير الدولية. د- يتم إبلاغها إلى أصحاب المصلحة المعنيين.
(4)	أن تتضمن سياسة الأمن السيبراني ما يلي: أ- تعريفاً لمفهوم الأمن السيبراني. ب- الأهداف العامة للأمن السيبراني ونطاق تطبيقها في الجهة. ج- توجهات مجلس الإدارة الداعمة لأهداف الأمن السيبراني. د- تحديد المسؤوليات العامة والخاصة المتعلقة بالأمن السيبراني. هـ- الإشارة إلى المعايير والإجراءات الداعمة للأمن السيبراني. و- متطلبات الأمن السيبراني التي تضمن ما يلي: i. تصنيف المعلومات بما يعكس أهميتها للجهة.

	ii. حماية المعلومات وفقاً لمتطلبات الأمن السيبراني ووفقاً لمستوى تقبل المخاطر. iii. تحديد مسؤولين (مالكين) لكافة أصول المعلومات. iv. إجراء تقييمات لمخاطر الأمن السيبراني الخاصة بأصول المعلومات. v. رفع مستوى الوعي لدى أصحاب المصلحة المعنيين بشأن الأمن السيبراني وسلوكهم المتوقع (من خلال برنامج التوعية بالأمن السيبراني). vi. الإلتزام بالمتطلبات التنظيمية والتعاقدية ذات الصلة. vii. الإبلاغ عن خروقات الأمن السيبراني ونقاط الضعف المشتبه بها. viii. دمج اعتبارات الأمن السيبراني ضمن إدارة استمرارية الأعمال.
6.4	**أدوار ومسؤوليات الأمن السيبراني (Roles Responsibilities of Cybersecurity)**
المبدأ	تحديد الأدوار والمسؤوليات لمنع التداخل والإزدواجية.
الهدف	ضمان وعي أصحاب المصلحة المعنيين بمسؤولياتهم المتعلقة بالأمن السيبراني، وتطبيق ضوابط الأمن السيبراني في جميع أقسام الجهة من خلال هيكل حوكمة واضح ومتكامل.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	**مجلس الإدارة :** يكون مسؤولاً عن: أ- التأكد من تخصيص ميزانية كافية للأمن السيبراني. ب- الموافقة على ميثاق لجنة الأمن السيبراني. ج- التصديق، بعد موافقة لجنة الأمن السيبراني، على ما يلي: i. حوكمة الأمن السيبراني. ii. استراتيجية الأمن السيبراني. iii. سياسة الأمن السيبراني.
(2)	**لجنة الأمن السيبراني:** تكون مسؤولة عن: أ- مراقبة ومراجعة وإبلاغ مدى تقبل الجهة لمخاطر الأمن السيبراني بشكل دوري، أو عند حدوث تغييرات جوهرية. ب- مراجعة استراتيجية الأمن السيبراني لضمان توافقها مع أهداف الجهة.

	ج- الموافقة على العناصر التالية، والتواصل بشأنها، ودعمها، ومراقبتها: i. حوكمة الأمن السيبراني. ii. استراتيجية الأمن السيبراني. iii. سياسة الأمن السيبراني. iv. برامج الأمن السيبراني (مثل: برنامج التوعية، تصنيف البيانات، حماية الخصوصية، منع تسرب البيانات، التحسينات السيبرانية الرئيسية). v. عملية إدارة مخاطر الأمن السيبراني. vi. مؤشرات المخاطر الرئيسية (KRIs) ومؤشرات الأداء الرئيسية (KPIs).
(3)	**الإدارة العليا:** تكون مسؤولة عن: أ- التأكد من أن المعايير والإجراءات تعكس متطلبات الأمن السيبراني (عند الإقتضاء). ب- التأكد من التزام الموظفين بسياسة الأمن السيبراني والمعايير والإجراءات ذات الصلة عند إصدارها أو تحديثها. ج- إدراج مسؤوليات الأمن السيبراني ضمن الأوصاف الوظيفية للوظائف الرئيسية والوظائف المتخصصة في الأمن السيبراني. د- التأكد من أن فرق المشاريع تتضمن موظفي الأمن السيبراني خلال مراحل التخطيط، التحليل، التصميم، والإختبار قبل إطلاق أي مشروع.
(4)	**مسؤول الأمن السيبراني** : يكون مسؤولاً عن: أ- تطبيق ومتابعة: i. استراتيجية الأمن السيبراني. ii. سياسة الأمن السيبراني. iii. بنية الأمن السيبراني. iv. عملية إدارة مخاطر الأمن السيبراني. ب- التأكد من إعداد واعتماد وتنفيذ المعايير والإجراءات الأمنية المفصلة. ج- تقديم حلول أمن سيبراني قائمة على المخاطر تغطي الجوانب البشرية والعملية والتقنية.

	د- تطوير الكوادر المتخصصة بالأمن السيبراني لتقديم حلول فعالة متوافقة مع بيئة الأعمال. هـ- الإشراف على أنشطة الأمن السيبراني في كافة أرجاء المنظمة، بما يشمل: i. مراقبة أنشطة الأمن السيبراني (مثل مركز العمليات الأمنية). ii. مراقبة مدى الإلتزام بالأنظمة والسياسات والمعايير والإجراءات السيبرانية. iii. الإشراف على التحقيقات في الحوادث السيبرانية. iv. جمع وتحليل معلومات التهديد من مصادر داخلية وخارجية. v. تنفيذ مراجعات الأمن السيبراني. و- إجراء تقييمات لمخاطر الأمن السيبراني على أصول المعلومات في الجهة. ز- دعم الوحدات الأخرى فيما يخص الأمن السيبراني، بما في ذلك: i. تصنيف المعلومات والأنظمة. ii. تحديد المتطلبات السيبرانية للمشاريع الحيوية. iii. إجراء مراجعات الأمن السيبراني. ح- تصميم وتنفيذ برامج التوعية بالأمن السيبراني. ط- قياس مؤشرات الأداء الرئيسية (KPIs) ومؤشرات المخاطر الرئيسية (KRIs) والإبلاغ عنها، وتشمل: i. تنفيذ استراتيجية الأمن السيبراني. ii. الإمتثال لسياسة الأمن السيبراني. iii. مدى الإلتزام بالمعايير والإجراءات. iv. فعالية برامج الأمن السيبراني المختلفة.
(5)	المراجعة الداخلية مسؤولة عن إجراء عمليات تدقيق دورية ومستقلة للأمن السيبراني.
(6)	جميع موظفي الجهة مسؤولون عن الإلتزام بسياسة الأمن السيبراني والمعايير والإجراءات المرتبطة بها.
6.5	**الأمن السيبراني في إدارة المشاريع (Cybersecurity in Project Management)**
المبدأ	تضمين الأمن السيبراني في حوكمة وإدارة المشاريع.
الهدف	ضمان تلبية جميع مشاريع الجهة لمتطلبات الأمن السيبراني.

الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	دمج الأمن السيبراني في منهجية إدارة المشاريع المعتمدة لدى الجهة لضمان تحديد ومعالجة مخاطر الأمن السيبراني ضمن نطاق المشروع.
(2)	أن تضمن منهجية إدارة المشاريع لدى الجهة ما يلي: أ- تضمين أهداف الأمن السيبراني ضمن الأهداف العامة للمشروع. ب- إشراك وظيفة الأمن السيبراني في جميع مراحل المشروع. ج- إجراء تقييم للمخاطر في المرحلة الإبتدائية للمشروع لتحديد مخاطر الأمن السيبراني، وضمان معالجتها إما من خلال الضوابط السيبرانية القائمة (إستناداً إلى المعايير المعتمدة) أو من خلال تطوير ضوابط جديدة. د- تسجيل مخاطر الأمن السيبراني في سجل مخاطر المشروع وتتبعها. هـ- تحديد وتوزيع المسؤوليات المتعلقة بالأمن السيبراني بوضوح. و- إجراء مراجعة مستقلة للأمن السيبراني من قبل جهة داخلية أو خارجية محايدة.
6.6	**تدريب الأمن السيبراني (Cybersecurity Training)**
المبدأ	تزويد موظفي الجهة بالتدريب اللازم حول كيفية تشغيل الأنظمة وتطبيقها والتعامل مع ضوابط الأمن السيبراني بشكل آمن.
الهدف	ضمان تمتع موظفي الجهة بالمهارات والمعرفة المطلوبة لحماية أصول معلوماتها والوفاء بمسؤولياتهم المتعلقة بالأمن السيبراني.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	توفير تدريب متخصص أو متعلق بمهارات الأمن السيبراني لفئات الموظفين العاملين في المجالات الوظيفية ذات الصلة داخل الجهة، بما يتماشى مع توصيف وظائفهم، ويشمل ذلك: أ- أصحاب الأدوار الرئيسية داخل الجهة. ب- موظفي وحدة الأمن السيبراني. ج- الموظفين المشاركين في تطوير أصول المعلومات وصيانتها فنياً. د- الموظفين المشاركين في عمليات تقييم المخاطر.

(2)	توفير التعليم اللازم لتزويد الموظفين بالمهارات والمعرفة المطلوبة لتشغيل أصول معلومات الجهة بشكل آمن.

7. إدارة المخاطر السيبرانية (Cyber Risk Management)

7.1	تقييم وإدارة مخاطر الأمن السيبراني (Cybersecurity Risk Assessment and Management)
المبدأ	تقييم المخاطر وإعتمادها وتنفيذها لتتوافق مع إدارة المخاطر العامة وأهداف الجهة.
الهدف	تحديد وتحليل وتقييم المخاطر السيبرانية المحتملة وتحديد أولوياتها واتخاذ قرارات سليمة لتخفيف تلك المخاطر.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تكون عملية تقييم مخاطر الأمن السيبراني: أ- مُعرفة. ب- معتمدة. ج- متوافقة مع المخاطر المؤسسية للجهة. د- متوافقة مع المعايير الدولية.
(2)	أن تكون المخاطر السيبرانية التي يمكن للجهة التعامل معها وتحملها محددة بوضوح ومعتمده رسمياً.
(3)	أن تركز إدارة مخاطر الأمن السيبراني علي حماية الآتي: أ- سرية المعلومات. ب- نزاهة المعلومات. ج- توفر المعلومات.
(4)	توثيق وتقييم مخاطر الأمن السيبراني بحيث تحوي: أ- تحديد المخاطر. ب- تحليل المخاطر. ج- الإستجابة للمخاطر. د- مراقبة المخاطر.

(5)	أن يتناول تقييم مخاطر الأمن السيبراني معلومات الجهة وأصولها المعلوماتية بما في ذلك على سبيل المثال لا الحصر العمليات التشغيلية، الأصول، المعالجات، والتطبيقات المستخدمة.
(6)	أن يكون التقييم السنوي لمخاطر الأمن السيبراني مستقلاً عن تقييم المخاطر الذي ينبغي إجرائه اثناء: أ- الحصول على أو تطوير أنظمة أو خدمات جديدة. ب- الصيانة الرئيسية للأنظمة الحالية أو الخدمات. ج- اختبار الأنظمة الجديدة والخدمات. د- بداية المشاريع. هـ- الإستعانة بمصادر خارجية لمشاريع جديدة أو خدمات قائمة.
(7)	أن تشمل أنشطة تقييم مخاطر الأمن السيبراني الوظائف التالية: أ- أعمال الجهة. ب- تكنولوجيا المعلومات. ج- الأمن السيبراني. د- المستخدمين الرئيسيين.
(8)	إضافة مخاطر الأمن السيبراني المحددة إلى خطة معالجة المخاطر.
(9)	توثيق وتسجيل خطة معالجة المخاطر بما في ذلك التحليل والضوابط المطبقة.
(10)	على مسؤولي المخاطر: أ- مراجعة تقرير تقييم المخاطر ووثائق خطة معالجة المخاطر مرة سنوياً علي الأقل. ب- ضمان استمرار فعالية الضوابط المطبقة وكفايتها. ج- التوصية باجراءات لتحسين الضوابط المطبقة.
(11)	إرسال تقرير تقييم المخاطر وخطة معالجة المخاطر سنوياً إلى الإدارات ذات الصلة والمديرين التنفيذيين داخل الجهة.
7.2	**منهجية تقييم مخاطر الأمن السيبراني (Cybersecurity Risk Assessment (Methodology**
المبدأ	استخدام منهجية لتقييم مخاطر الأمن السبراني لتحديد مدي التهديدات المحتمله والمرتبطة بالمعلومات.

الهدف	الحصـول على تقرير لتقييم المخاطر السـيبرانية الذي يسـاعد علي تحديد الضـوابط المناسبة للتخفيف من تلك المخاطر إلى مستوي مقبول.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تكون منهجية تقييم المخاطر متوافقة مع المعايير الدولية والضوابط الصادره عن بنك السودان المركزي.
(2)	أن تكون المنهجية معتمدة من مجلس الإداره ويتم مراجعتها بصورة دورية.
(3)	تحديد الغرض من تقييم المخاطر.
(4)	تحديد نطاق تقييم المخاطر.
(5)	تحديد الإفتراضات والقيود مثل :المالية والزمنية والتشغيلية والتقنية، وغيرها.
7.3	**تحديد مخاطر الأمن السيبراني (Cybersecurity Risk Identification)**
المبدأ	تحديد وتصـنيف المخاطر والتهديدات المحتملة المرتبطة بالأمن السـيبراني داخل أنظمة الجهة وشبكتها وتطبيقاتها وبياناتها، وغيرها.
الهدف	تحديد نقاط الضعف أو الثغرات واحتمالية إستغلالها في هجمات سيبرانية، كما يساعد تحديد الأصول في تتبع الأصول وحالتها وتقييم المخاطر المرتبطة بالأصل علي أساس دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد الأصول وتوثيقها عن طريق الآتي: أ- جرد الأصول. ب- مراقبة الأصول. ج- الأمين المسؤول عن الأصول . د- مالك الأصول.
(2)	تحديد التهديدات وتوثيقها وتقييم مدى أهميتها مع الأخذ في الإعتبار مصـادرها التي تتمثل في الآتي: أ- المعلومات التي تم جمعها من مصادر مشبوهة وادخالها إلى الجهة. ب- المعلومـات التي تم جمعهـا من الأحـداث العـارضـــه ومـالكي الأصـــول والمستخدمين. ج- أحداث التهديدات التي تتميز بالتكتيكات والتقنيات والإجراءات.

(3)	تحديد وتوثيق الثغرات الأمنية، عبر الإحتفاظ بتقرير الثغرات الأمنية الناتج عن نظام إدارة الثغرات وإدراجها كجزء من عملية تحديد المخاطر.
(4)	تحديد وتوثيق المسؤولين عن إدارة مخاطر الأمن السيبراني(Risk Owners).
7.4	**تحليل مخاطر الأمن السيبراني (Cybersecurity Risk Analysis)**
المبدأ	جمع وتحليل البيانات من مختلف المصادر لتحديد التهديدات ونقاط الضعف، لاكتشاف الهجمات والإستجابة لها بفعالية عبر تطبيق استراتيجيات إستباقية وإجراءات دفاعية متعددة.
الهدف	تحليل مخاطر الأمن السيبراني وفحص كل خطر على أنظمة المعلومات والأجهزة والبيانات الخاصة بالجهة وتحديد التهديدات المحتمله مسبقاً.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تقييم العواقب التي من المحتمل أن تنتج من حدوث خطر محدد.
(2)	تحديد أولويات الخطر.
(3)	تخصيص الموارد للمخاطر المحددة.
7.5	**الإستجابة لمخاطر الأمن السيبراني (Cybersecurity Risk Response)**
المبدأ	تقييم وتحديد مستوي الإستجابة المناسب للمخاطر المحددة.
الهدف	وضع خطة وإجراءات منظمة للتعامل مع الحوادث الأمنية السيبرانية المحتملة أو التي حدثت بالفعل، بهدف تقليل الأضرار واستعادة العمليات الطبيعية، لمنع تكرار الحادث مستقبلاً.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد الإستجابة المناسبة: أ- **القبول**: إذا كان مستوى المخاطر يفي بمعايير قبول المخاطر. ب- **الرفض**: عندما تعتبر المخاطر المحددة مرتفعة جداً أو عندما تتجاوز تكلفة تطبيق معالجة المخاطر الفوائد المرجوة. ج- **التخفيف** : تقليل مستوي المخاطر من خلال اختيار الضوابط.

	د- **النقل** : يتم نقل المخاطر إلى طرف آخر يمكنه إدارة المخاطر بشكل فعال بناءً على تقييم المخاطر.
(2)	تحديد الضوابط ذات الصلة : أ- **أنواع الحماية**: تتمثل أنواع الحماية في التصحيح ،الوقاية ،الردع ، الكشف،الإسترداد، الازالة،تقليل التأثير،المراقبة، والتوعية. ب- **خيارات اختيار الضوابط** : الإستحواذ، التنفيذ، الإدارة، التشغيل، الرقابة، والصيانة. ج- يجوز للجهات موازنة تكلفة الضوابط مقابل قيمة الأصول المحمية. د- يجب إعادة النظر في جميع المخاطر المتبقية كلما تمت مراجعة تقييم المخاطر أو تم اكتشاف تهديد جديد.
7.6	**مراقبة مخاطر الأمن السيبراني (Cybersecurity Risk Monitoring)**
المبدأ	مراقبة وإدارة المخاطر السيبرانية باستمرار من خلال اكتشاف التهديدات ومعالجة نقاط الضعف، تسهيل الإستجابة للحوادث ، ضمان الإلتزام ، والتحسين المستمر في ممارسات الأمن في الجهة.
الهدف	جمع وتحليل مؤشرات التهديدات السيبرانية المحتملة، وضع خطة للتصدي لها باستخدام التقنيات والأدوات الحديثة ، ثم تصنيف هذه التهديدات بالإجراءات المناسبة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	المراقبة المستمرة للتهديدات ونقاط الضعف وإحتمالية حدوثها وتأثيرها وقيمة الأصول.
(2)	تحديد أولويات معالجة المخاطر.
(3)	مراقبة فعالية الضوابط.
(4)	تتبع تقدم خطة معالجة المخاطر.
(5)	توثيق جميع إجراءات معالجة مخاطر الأمن السيبراني .
(6)	مراجعة واعتماد إجراءات معالجة مخاطر الأمن السيبراني.

8. الضوابط الفنية والتشغيلية (Technical and Operational Controls)

8.1	إدارة الأصول (Asset Management)
المبدأ	إدارة جميع الأصول بناءً على قيمتها وأهميتها وسريتها وتأثيرها على العمليات في حالة تعطلها أو اختراقها، بالإضافة إلى تحديد ملكية واضحة لكل أصل.
الهدف	ضمان أن يكون للجهة مخزون دقيق ومحدث ورؤية مركزية للموقع المادي والمنطقي والتفاصيل ذات الصلة بجميع أصول المعلومات المتاحة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أ- تحديد عملية إدارة الأصول واعتمادها وتنفيذها من أجل دعم عملياتها ،علي سبيل المثال لا الحصر (العمليات المالية والمشتريات وتقنية المعلومات والأمن السيبراني). ب- الحفاظ على سجل دقيق وحديث لجميع الأصول (سجل الأصول). ج- مراقبة فعالية عملية إدارة الأصول وقياسها وتقييمها دورياً. د- أن تشمل عملية إدارة الأصول ما يلي: i. ملكية أصول المعلومات وحراستها. ii. الإشارة إلى العمليات الأخرى ذات الصلة، اعتماداً على إدارة الأصول. iii. تصنيف أصول المعلومات، ووضع العلامات عليها، ومعالجتها. iv. اكتشاف أصول معلومات جديدة.
8.1.1	تحديد الأصول (Asset Identification)
المبدأ	تحديد وتصنيف أصول المعلومات بناءً على أهميتها وحساسيتها مع العمل و الإحتفاظ بجرد دوري للأصول.
الهدف	ضمان تحديد أصول المعلومات ووضع علامات عليها وحمايتها وتوصيلها إلى المستخدمين.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	الحفاظ على جرد كامل لأصول المعلومات، بما في ذلك الأجهزة والبرامج والتراخيص. ويعتبر هذا السجل أمراً بالغ الأهمية أثناء عمليات التدقيق والإستجابة للحوادث.
(2)	إصدار تعليمات بعدم ترك الأصول خارج المبنى دون مراقبة عند الإنتهاء من العمل بها.

(3)	دراسة وتطبيق الضوابط الفنية والمادية، مثل تشفير الأقراص، وتقنيات المسح عن بُعد والقفل عند الإنتهاء من العمل بها.
(4)	اغلاق أي أصل غير مراقب أو عام للإستخدام المخصص له فقط، مع ضمان عدم إمكانية الوصول غير المصرح به إلى مكوناته المادية والمنطقية.
(5)	وضع الأصول غير المراقبة في وضع إيقاف التشغيل بعد ساعات العمل.
8.1.2	**الموارد البشرية (Human Resource Management)**
المبدأ	دمج متطلبات الأمن السيبراني في عمليات الموارد البشرية.
الهدف	ضمان تضمين مسؤوليات الأمن السيبراني لموظفي الجهة في اتفاقيات الموظفين ويتم فحص الموظفين قبل وأثناء دورة حياتهم المهنية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أ- أن تُحدد عملية الموارد البشرية متطلبات الأمن السيبراني، وتُعتمد وتُنفذ. ب- مراقبة فعالية عملية الموارد البشرية وقياسها وتقييمها دورياً. ج- أن تشمل عملية الموارد البشرية ما يلي: i. مسؤوليات الأمن السيبراني وبنود عدم الإفصاح في اتفاقيات الموظفين (أثناء وبعد التوظيف) ii. أن يتلقى الموظفون وعياً بالأمن السيبراني في بداية عملهم وأثناءه. iii. متى ستكون الإجراءات التأديبية سارية. iv. الفحص والتحقق من الخلفية. v. أنشطة الأمن السيبراني بعد انتهاء الخدمة وفق الآتي: a. إلغاء حقوق الوصول. b. إعادة أصول المعلومات المخصصة علي سبيل المثال لا الحصر (حقوق الوصول، والرموز، والأجهزة المحمولة، وجميع المعلومات الإلكترونية والمادية).
(2)	وضع وتطبيق والحفاظ على سياسة الاستخدام المقبول لأصول المعلومات. وأن تتضمن هذه السياسة على الأقل ما يلي: أ- المسؤوليات المتعلقة بالملكية الفكرية والمعلومات المحمية بحقوق الطبع والنشر.

	ب- شروط منح الوصول إلى المعلومات السرية، بالإضافة إلى المسؤوليات المتعلقة بتصنيف ومعالجة ونقل أصول المعلومات، سواءً المملوكة للجهة أو المستلمة من طرف خارجي. ج- المسؤوليات المتعلقة بحسابات المستخدمين. د- المسؤوليات المتعلقة باستخدام الإنترنت والبريد الإلكتروني الرسمي. هـ- المسؤوليات المتعلقة بتنظيف الشاشات والمكاتب. و- مسؤولية إلزام جميع الموظفين والموظفين المؤقتين والمتعاقدين بإعادة الأصول عند انتهاء خدمتهم. ز- المسؤوليات المتعلقة بالإبلاغ عن الأنشطة المشبوهة المرصودة. ح- المسؤوليات المتعلقة بالتصريحات العامة.
8.1.3	**أصول البرمجيات (Software Assets)**
المبدأ	تحديد ملكية الأصول، وتفويضات الملكية، والمسؤول عن الحفظ، والمستخدمين لأصول البرمجيات.
الهدف	إجراء جرد للبرامج والمنصات والتطبيقات الجاهزة والمطورة داخلياً.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد مواقع الأصول، سواءً على مستوى الجهة أو على السحابة.
(2)	تحديد الإصدارة، والنسخة.
(3)	جرد وتحديد وظائف العمل ، والدور والمكانة في البيئة من حيث الاتي: أ- الإنتاج، التطوير، الإختبار، وغيرها. ب- المشرف الإفتراضي، نظام التشغيل، نظام إدارة قواعد البيانات ، (تطبيقات الأعمال، طبقة الوصول، البرامج الوسيطة)، وغيرها. ج- خدمات البنية التحتية، وحدة التحكم الإدارية (Administrative console) ، بوابة التطبيقات (Applications portal)، واجهة الربط (API) بين تطبيقات الخدمات وتطبيقات الهاتف المحمول، وغيرها. د- تطبيق أو برنامج العميل، تطبيق الهاتف المحمول، وغيرها. هـ- البرامج الثابتة والبرامج الداعمة الأساسية Firmware and basic support (software). و- أنواع البيانات المخزنة والمعالجة لكل نظام. وتشمل بيانات الأعمال الأساسية، ومعلومات تحديد الهوية الشخصية، وبيانات الأعمال الداعمة، والبيانات المالية، وغيرها.

	ز- المعلومات الفنية حول النظام علي سبيل المثال لا الحصر (عناوين IP الداخلية، وحالة الوصول إلى الإنترنت، وحالة التعامل مع الجمهور، وعناوين IP المنشورة للاستخدام الخارجي). ح- تاريخ انتهاء الصلاحية ونهاية الدعم للنظام.
(4)	يُمكن الاحتفاظ بقوائم مُجمّعة للبرامج المُثبّتة على نطاق واسع.
(5)	التواصل الجيد والمراجعة المُستمرة عند التغيير وبشكل مُنتظم.
8.1.4	**تصنيف البيانات (Data Classification)**
المبدأ	وضع تصنيف يسهم في منع غير المصرح به للوصول الي البيانات الحساسة.
الهدف	إجراء عملية تصنيف البيانات بانتظام، لمنع الآثار المترتبة على فقدان السرية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إجراء عملية تصنيف البيانات بانتظام، مع مراعاة الأثر المحتمل وتكلفة العواقب المترتبة على فقدان السرية.
(2)	تصنيف البيانات وفقاً للقوانين واللوائح السارية.
(3)	تصنيف البيانات إلى أربع فئات على الأقل في سياق (البيانات العامة، والاستخدام الداخلي، والسرية، والسرية للغاية).
(4)	أن تكون البيانات مصنفة جيداً، وأن تُراجع باستمرار وبشكل دوري، وعند التغيير.
(5)	تصنيف أصول البيانات وترتيب أولوياتها بناءً على قيمتها الإجمالية.
(6)	استخدام نهج شبه كمي للتعبير عن القيمة الإجمالية للأصول.
(7)	التواصل الجيد والمراجعة المستمرة، سواءً على أساس التغيير أو بشكل دوري.
8.2	**الوقاية والكشف (Prevention and Detection)**
8.2.1	**الأمن المادي (Physical Security)**
المبدأ	حماية جميع المرافق التي تستضيف أصول المعلومات مادياً ضد الأحداث الأمنية المتعمدة وغير المتعمدة.
الهدف	وضع اجراءات لمنع الوصول المادي غير المصرح به إلى أصول المعلومات ولضمان حمايتها.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	تحديد المواقع والمناطق الآمنة التي تحتوي على مرافق لتخزين أو معالجة أو نقل المعلومات الحساسة و/أو الهامة. ويشمل ذلك - على سبيل المثال لا الحصر - مراكز البيانات، المكاتب، الغرف، مواقع نقاط الوصول، أجهزة شبكات الوصول، ومسارات خطوط الاتصالات.
(2)	مراقبة فعالية عملية الأمن المادي، وقياسها، وتقييمها دورياً.
(3)	أن تشمل عملية الأمن المادي،على سبيل المثال لا الحصر: أ- ضوابط الدخول المادية، بما في ذلك أمن الزوار. ب- المراقبة والرصد (مثل كاميرات المراقبة المرئية، وتتبع أجهزة الصراف الآلي بنظام تحديد المواقع العالمي (GPS)، وأجهزة استشعار الحساسية والإنذار المبكر). ج- حماية مراكز البيانات وغرف البيانات. د- حماية البيئة. هـ- حماية أصول المعلومات أثناء دورة حياتها، بما في ذلك النقل والتخلص الآمن منها، وتجنب الوصول غير المصرح به وتسريب البيانات (غير المقصود). و- التمييز بين الموظفين في الموقع، والموظفين المؤقتين، والزوار، والضيوف. ز- تحديد هوية الموظفين المؤقتين، والزوار، والضيوف، وتفويضهم قبل دخول الأماكن والمناطق الآمنة، والتأكد من حراستهم طوال الوقت. ح- انتهاء صلاحية بطاقات الهوية الممنوحة للموظفين المؤقتين، والزوار، والضيوف. ط- جمع بطاقات الهوية قبل مغادرة المنشأة أو عند انتهاء صلاحيتها.
8.2.1.1	**حماية البيئة المادية للتشغيل (Protection of the Physical Operating Environment)**
المبدأ	مراعاة الظروف البيئية والإضطرابات ودمجها في تصميم وبناء المنشآت، بما في ذلك مناطق المهام الآمنة والحيوية.
الهدف	تطبيق ضوابط مراقبة وكشف وحماية مستمرة للمناطق الآمنة ومواقع المهام الحيوية من المخاطر البيئية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	ضمان الإلتزام بتوصيات السلامة وإرشاداتها ولوائحها الخاصة بقوانين المباني/المنشآت.

(2)	مراعاة الظروف البيئية والإضطرابات ودمجها في تصميم وبناء المنشآت، بما في ذلك مناطق المهام الآمنة والحيوية.
(3)	دراسة وتطبيق ضوابط الأمن السيبراني المعمول بها على جميع ضوابط وأنظمة الإدارة البيئية المدعومة بتكنولوجيا المعلومات.
(4)	تطبيق ضوابط مراقبة وكشف وحماية مستمرة للمناطق الآمنة ومواقع المهام الحيوية من المخاطر البيئية، بما في ذلك انقطاع التيار الكهربائي، ودرجة الحرارة، والرطوبة، وتسربات المياه.
(5)	وضع خطط الإخلاء، والتواصل بشأنها، واختبارها، ومراجعتها بشكل دوري.
8.2.1.2	**المراقبة المستمرة (Continuous Monitoring)**
المبدأ	الإحتفاظ بسجلات دخول المنشأة وأي مناطق أو مواقع آمنة محددة.
الهدف	أن يتم تسجيل جميع الأحداث الخاصة بالدخول والخروج للمنشاة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	الإحتفاظ بسجلات دخول المنشأة وأي مناطق أو مواقع آمنة محددة. وأن يحوي السجل ما يلي: أ- أسماء الزوار. ب- أوقات وتواريخ الدخول/الخروج. ج- الشركات المُستضافة.
8.2.2	**المرونة من خلال التصميم (Resilience Through Design)**
8.2.2.1	**بيئات التطوير والاختبار والإنتاج (Development, Testing, and Production Environments)**
المبدأ	حماية بيئات التطوير وعزلها بطريقة تضمن تقييد الوصول للأشخاص المصرح لهم فقط.
الهدف	تقييد الوصول للأشخاص المصرح لهم فقط.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تبقي بيئات التطوير والاختبار والإنتاج منفصلة على مستوى الشبكة ومستوى الوصول المنطقي، حيث: أ- يُطبَّق الفصل من خلال التحكم في الوصول. ب- لا يُسمح للمطورين بالوصول إلى بيئة الإنتاج.

	ج- يجب أن يخضع فصل المهام بين البيئات، ومستويات التفويض لنقل التغييرات والعناصر من بيئة إلى أخرى، لنتائج تقييم المخاطر.
(2)	حماية بيئات التطوير وعزلها بطريقة تضمن على الأقل: أ- تقييد الوصول للأشخاص المصرح لهم فقط، مع النشر المباشر المُتحكم به عبر الإنترنت عند الحاجة فقط. ب- تطبيق ضوابط لضمان عدم وجود أي تطوير أو تحديث ضار أو عرضي قد يُشكل ثغرات أمنية. ج- فرض رقابة صارمة على تعديلات حزم البرامج أو التخصيصات داخل الحزمة لضمان عدم التأثير سلباً على السلامة الداخلية أو أمان التطبيق. د- منع استخراج البيانات والشيفرة المصدرية من البيئة. هـ- ضمان مراقبة نشاط المطورين، سواءً كانوا موظفين أو مؤقتين.
(3)	تطبيق ذلك على بيئات التطوير سواء المحلية أو السحابية على سبيل المثال لا الحصر(Cloud DevOps).
(4)	اختبار التطورات والإصدارات الجديدة بدقة في بيئة الاختبار وقبل الاختبار. يجب تصميم وتطوير سيناريوهات ومعايير الاختبار بناءً على متطلبات العمل والتشغيل والأمن.
(5)	على المدير المسؤول عن إدارة الأمن السيبراني وصاحب العمل قبول نتائج الاختبار الخاصة بكل منهما.
(6)	في بيئات الإنتاج، وبناءً على نتائج تقييم المخاطر، يجب على الجهة تنفيذ وظيفة رئيسية واحدة لكل مثيل حوسبة.
(7)	إزالة أي بيانات اختبار وشيفرة مصدر من النظام قبل تشغيله في بيئة الإنتاج.
(8)	ألا تستخدم بيانات الإنتاج لأغراض الاختبار أو التطوير. ويجب حظر نقل البيانات والمعلومات السرية خارج محتوي الإنتاج إلى بيئة أخرى أو إلى محركات أقراص ثابتة محلية أو وسائط قابلة للإزالة أو التخزين السحابي إلا بتصريح صريح من الجهه والمدير المسؤول عن إدارة الأمن السيبراني بناءً على احتياجات العمل المحددة، مع مراعاة إخفاء هوية البيانات قدر الإمكان.
(9)	التأكد من أن مستوى أمان بيئة الاختبار هو نفس مستوى الأمان في بيئة الإنتاج قبل نقل أي بيانات ومعلومات سرية.

8.2.2.2	دورة حياة التطوير الأمنة (Secure Development Lifecycle)
المبدأ	تحديد عملية إدارة دورة حياة تطوير آمنة والحفاظ عليها لضـمان تلبية متطلبات الأمان خلال جميع مراحل دورة حياة تطوير البرمجيات أو اقتناء برمجيات جديدة.
الهدف	ضـمان تلبية متطلبات الأمان خلال جميع مراحل دورة حياة تطوير البرمجيات أو اقتناء برمجيات جديدة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد عملية إدارة دورة حياة تطوير آمنة والحفاظ عليها لضـمان تلبية متطلبات الأمان خلال جميع مراحل دورة حياة تطوير البرمجيات أو اقتناء برمجيات جديدة. وبغض النظر عن منهجية تطوير البرمجيات المعتمدة، يجب أن تأخذ العملية في الإعتبار ما يلي: أ- تحديد حالات إساءة الاستخدام خلال مرحلة جمع المتطلبات، بالإضافة إلى متطلبات الأمن السيبراني والخصوصية. ب- إجراء عملية تقييم مخاطر الأمان لتحديد الجوانب التي تتطلب نمذجة التهديدات (Threat Modelling) ومراجعة تصميم الأمان. ج- على الجهة خلال مرحلة البنية والتصميم: i. ضمان وضع متطلبات محددة للأمان والخصوصية. ii. إجراء عمليات تحليل لأنواع الهجوم ونمذجة التهديدات لتحديد نقاط الضعف والتهديدات المحتملة، بالإضافة إلى وضع إجراءات التخفيف المناسبة. iii. تُحدد إدارة مراقبة الجودة سـيناريوهات ومعايير الإختبار القائمة على المخاطر.
(2)	على المطورين خلال مرحلة / مراحل التنفيذ والترميز مراعاة مبادئ وممارسـات الترميز الآمنة المعتمدة، كما يجب إجراء تحليل ثابت للكود عبر مراجعة الكود.
(3)	إجراء تحليل ديناميكي للكود (عبر فحص الثغرات الأمنية واختبار الاختراق)، خلال مرحلة/مراحل الاختبار والتحقق، كما يجب إجراء حالات وسيناريوهات اختبار، ومراجعة النتائج ومعالجتها.
(4)	إجراء عمليات أمنية محددة، بعد الإصدار.

(5)	ترتيب اتفاقيات الضمان مع المورد لإدارة الكود المصدري، بالنسبة للتطبيقات الهامة المكتسبة.
8.2.2.3	الترميز الآمن للكود المصدري (Secure Coding of Source Code)
المبدأ	مراجعة الشيفرة المصدرية قبل إصدارها في بيئة الإنتاج لضمان توافقها مع المبادئ والممارسات المعتمدة، ولتحديد أي نقاط ضعف مُكتشفة ومعالجتها.
الهدف	ضمان تحديد أي نقاط ضعف مُكتشفة ومعالجتها في الشيفرة المصدرية قبل إصدارها في بيئة الإنتاج.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إنشاء عملية تواصل جيدة والحفاظ عليها لضمان قيام المطورين للتطبيقات الداخلية (سواء الموظفين أو الموظفين المؤقتين) بما يلي: أ- مراعاة مبادئ تصميم الأمن في جميع مراحل التطوير. يجوز للجهة اعتماد إحدى أفضل الممارسات الدولية (مثل مبادئ OWASP). ويجب أن تراعي أي ممارسة معتمدة المبادئ التالية كحد أدنى: i. قصر وظائف التطبيق المعرضة للخطر على المستخدمين المسجلين أو المعتمدين فقط. ii. تفعيل جميع ميزات أمان التطبيق المتاحة افتراضياً. iii. تطبيق إعدادات افتراضية آمنة من خلال منع اتخاذ إجراء للسلوكيات غير المحددة وضمان "فشل" التطبيق في حالة آمنة. iv. تطبيق مبدأ الحد الأدنى من الامتيازات من خلال منح الحد الأدنى من الصلاحيات اللازمة للمستخدمين لأداء المهام وفقاً لأدوارهم في العمل. v. تطبيق مبدأ فصل المهام من خلال تعيين أدوار لكل مجموعة من مهام التطبيق ذات الصلة، وضمان القضاء على التداخل غير المبرر بين الأدوار المختلفة. vi. تطبيق مبدأ الدفاع المتعمق بالاعتماد على ضوابط أمنية متعددة للتخفيف من المخاطر المحددة بطرق مختلفة.

	vii. التحقق من صحة كل محاولة وصول، وكذلك جميع البيانات الواردة، من خدمات الجهات الخارجية بافتراض عدم وجود ثقة. viii. ألا يعتمد تأمين التطبيقات على إخفاء الوظائف الأساسية أو شيفرة المصدر أو المفاتيح أو السلاسل. ix. مراعاة استخدام هياكل وآليات بسيطة وغير معقدة، عند تطوير ضوابط الأمان x. ألا يُصعّب استخدام خدمات التطبيقات المُقدّمة. xi. تحديد السبب الجذري والأنظمة الأخرى المتأثرة واختبار الحلول المُعالجة بدقة قبل إطلاقها في الإنتاج في حال اكتشاف أي مشكلة أمنية في أي تطبيق. ب- تطبيق آليات وتقنيات تشفير آمنة. يمكن للجهة اعتماد إحدى أفضل الممارسات الدولية (مثل ممارسات التشفير الآمنة OWASP). التي تستخدم لمعالجة على الأقل المخاطر والعيوب ونقاط الضعف المحددة في "أخطر عشرة مخاطر أمنية لتطبيقات الويب" وفقاً لـ OWASP و"أخطر 25 خطأً برمجياً" وفقاً لـ (CWE/SANS).
(2)	تسجيل أنشطة المستخدم (سواءً كانت ذات امتيازات أو عادية)، وجميع أحداث الوصول (على مستوى الشبكة والتطبيق)، وأي أحداث أخرى متعلقة بالأمن، بناءً على أهمية التطبيق وحساسيته،
(3)	تطبيق آليات حماية للسجلات المجمعة ومسارات التدقيق ضد التلاعب والوصول غير المصرح به والحذف.
(4)	تطبيق جميع التدابير الوقائية المحددة ضد تهديدات التطبيق في جميع أجزاء التطبيق ومكوناته، سواءً كانت متاحة للعامة أو مقيدة للمستخدمين المسجلين.
(5)	توضيح جميع متطلبات التشفير الآمن للتطبيقات الداخلية في اتفاقيات توريد التطبيقات التجارية الجاهزة. يجب على الجهة طلب شهادة أو دليل للتطبيقات التجارية الجاهزة لضمان إجراء اختبارات الأمان ومعالجة الثغرات الأمنية.
(6)	إجراء تدريب متخصص بانتظام للمطورين حول آليات وتقنيات التشفير الآمن وتجنب ثغرات التشفير الشائعة.

(7)	بناءً على نتائج تقييم المخاطر، يجب مراجعة الشيفرة المصدرية قبل إصدارها في بيئة الإنتاج لضمان توافقها مع المبادئ والممارسات المعتمدة، ولتحديد أي نقاط ضعف مُكتشفة ومعالجتها. يجب أن يُجري عملية المراجعة أفرادٌ غير المُبرمجين. بالنسبة للشيفرة المُستعانة بمصادر خارجية، يجب الحصول على شهادة مراجعة مستقلة.
8.2.2.4	**نمذجة التهديدات (Threat Modelling)**
المبدأ	إنشاء عملية مُتواصلة تخص إجراءات نمذجة التهديدات خلال مرحلة التصميم.
الهدف	تحديد نقاط الضعف والتهديدات المحتملة، ووضع ضوابط التخفيف.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحليل البنية التحتية إلى مخططات تدفق البيانات التفصيلية بالكامل والتي تتضمن: أ- محتويات معالجة البيانات، مثل حالات الحوسبة، والملفات القابلة للتنفيذ، والمكتبات الثابتة والديناميكية، وغيرها. ب- مخازن البيانات، مثل الملفات، وقواعد البيانات، وقوائم انتظار الرسائل، وغيرها. ج- تدفقات البيانات، علي سبيل المثال لا الحصر استدعاء إجراء عن بُعد (RPC)، واستدعاءات واجهة برمجة تطبيقات الويب، واستدعاءات نماذج الويب، وغيرها. د- الجهات الفاعلة، ونقاط الدخول، وحدود الثقة.
(2)	تحديد وتحليل التهديدات المحتملة التي قد تؤثر على سرية البيانات والمعلومات وسلامتها وتوافرها والمصادقة والتفويض والمساءلة وخصائص أمان عدم التنصل أثناء العمليات المختلفة ومراحل التخزين والنقل، وكذلك على مستوى الشبكة ونظام التشغيل والتطبيق. قد تشمل مصادر المعلومات المتعلقة بالتهديدات المحتملة ما يلي: أ- تبادل الأفكار لتحديد حالات إساءة الاستخدام وسيناريوهات الهجوم. ب- تاريخ الحوادث السابقة. ج- الموردون، ومقدمو الخدمات من جهات خارجية، ومكتبات تهديدات فرق الإستجابة لطوارئ الحاسبات.

	أساليب وتقنيات وإجراءات التهديد التي تتناولها مصادر عالمية مثل (OWASP) لأخطر عشرة مخاطر أمنية لتطبيقات الويب، و(CWE/SANS) لأخطر 25 خطأً برمجيا، و(CK&MITRE ATT) لتكتيكات وتقنيات المؤسسات والأجهزة المحمولة.
(3)	بناء سجل التهديدات الذي يحدد: أ- تكتيكات التهديد (الأهداف الفنية) والتقنيات ذات الصلة (كيفية تحقيق الأهداف) لكل تهديد مُحدد. ب- تقييم كل تكتيك وتقنية تهديد مُحددة باستخدام أحد نماذج تقييم المخاطر وأنظمة التسجيل القياسية علي سبيل المثال لا الحصر(DREAD، CVSS).
(4)	تحديد إجراءات لضمان تطبيق وتنفيذ مخرجات عملية نمذجة التهديدات والتدابير الوقائية الموصى بها.
8.2.3	**إدارة الهوية والمصادقة والتحكم في الوصول (Identity Management, Authentication, and Access Control)**
8.2.3.1	**إدارة الهوية (Identity Management)**
المبدأ	تقييد الوصول إلى أصول المعلومات الخاصة بها بما يتماشى مع متطلبات أعمالها على أساس مبادئ الحاجة إلى الإمتلاك أو الحاجة إلى المعرفة.
الهدف	ضمان أن الجهة توفر فقط امتيازات الوصول المسموح بها والكافية للمستخدمين المعتمدين فقط.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أ- تحديد سياسة إدارة الهوية والوصول، بما في ذلك المسؤوليات والمساءلات، والموافقة عليها وتنفيذها. ب- مراقبة الإلتزام بسياسة الهوية والوصول. ج- قياس فعالية ضوابط الأمن السيبراني ضمن سياسة إدارة الهوية والوصول وتقييمها دورياً. د- أن تضمن في سياسة إدارة الهوية والوصول ما يلي: i. متطلبات العمل للتحكم في الوصول (أي ما يجب توفره وما يجب معرفته). ii. إدارة وصول المستخدمين كما يلي:

	a. يجب تغطية جميع أنواع المستخدمين المحددة علي سبيل المثال لا الحصر (الموظفون الداخليون، والأطراف الثالثة) b. يجب أن تبدأ إدارة الموارد البشرية بتغييرات الحالة الوظيفية أو المناصب الوظيفية للموظفين الداخليين (المنضمون، والمنتقلون، والمغادرون). c. يجب أن تبدأ الجهة المسؤولة المعينة بتغييرات الموظفين الخارجيين أو الأطراف الثالثة. d. أن تتم الموافقة رسمياً على طلبات وصول المستخدم وفقًا لمتطلبات العمل والإلتزام، وضرورة الحصول عليها وضرورة معرفتها لتجنب الوصول غير المصرح به وتسريب البيانات (غير المقصود).
8.2.3.2	**إدراة الوصول (Access Management)**
المبدأ	تطبيق نظام مصادقة يتناسب مع مستوى المخاطر المرتبطة بعملية الوصول.
الهدف	ضمان تطبيق نظام مصادقة للأفراد والأجهزة والخدمات عند طلب الوصول إلى أصول وموارد المعلومات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	المصادقة متعددة العوامل للأنظمة والملفات الحساسة والحرجة.
(2)	تخصيص وتقييد استخدام الوصول المتميز والوصول عن بُعد، مع تحديد: أ- استخدام المصادقة متعددة العوامل لجميع عمليات الوصول عن بُعد. ب- استخدام المصادقة متعددة العوامل للوصول المتميز على الأنظمة الحرجة بناءً على تقييم المخاطر. ج- المراجعة الدورية للمستخدمين ذوي الحسابات المميزة ، ومن علي البعد. د- المساءلة الفردية. هـ- استخدام الحسابات المميزة غير الشخصية، وفق الاتي: i. التقييد والمراقبة. ii. تغيير كلمات المرور بشكل متكرر وفي نهاية كل جلسة.

	iii. أن تكون كلمات المرور المؤقتة والمخصصة للإستخدام مرة واحدة قصيرة الصلاحية، وأن تُرسل إلى عناوين مسجلة مسبقاً (أرقام الهواتف المحمولة وعناوين البريد الإلكتروني). iv. إخطار الأفراد بآخر وصول ناجح أو فاشل، وآخر إعادة تعيين لكلمة المرور. v. يمكن للمسؤولين تعيين كلمة مرور للاستخدام لأول مرة، ثم فرض تغييرها فوراً بعد الاستخدام الأول. vi. على المسؤول تجنب استخدام كلمات المرور الافتراضية والمعروفة، أو الاعتماد على كلمات مرور عشوائية يتم إنشاؤها تلقائياً. vii. أن يتمكن الأفراد كلما أمكن من اختيار كلمات مرورهم الخاصة. viii. تطبيق آليات قوية لتسجيل الدخول الفردي، مثل آليات مصادقة التحدي والإستجابة، وآليات مصادقة مشفرة قائمة على النماذج (مثلاً عبر إصدار آمن من TLS).
(3)	تأمين نقل بيانات المصادقة والجلسة ضد التلاعب والوصول غير المُصرّح به والاختراق.
(4)	مصادقة كل طلب وصول باستخدام مُعرّف جلسة أو رمز أو تذكرة صالحة.
(5)	تأمين بيانات الجلسة المُخزّنة على جانبي العميل والمخدم (Client / Server) ضد التلاعب والاختراق على الأقل.
(6)	مراقبة عمليات تسجيل الدخول المتزامنة للأفراد والحد منها.
(7)	إنهاء الجلسات غير النشطة بعد فترة مُحددة، بناءً على تقييم مدى أهمية وحساسية النظام والتطبيق والمعاملات المُتبادلة.
8.2.3.3	**إدارة حقوق الوصول (Access Rights Management)**
المبدأ	تحديد حقوق الوصول لكل عميل من خلال تحديد أصول المعلومات و/أو الموارد ومستوى الصلاحيات المطلوبة للوصول.
الهدف	يقتصر وصول الأفراد المُصادق عليهم على البيانات التي يملكونها والمسموح لهم بالوصول إليها فقط.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	أن يتطلب توفير حقوق الوصول للأفراد تبريراً وتفويضاً موثقاً من مالك أصل المعلومات أو المورد.
(2)	أن يقتصر وصول الأفراد المُصادق عليهم على البيانات التي يملكونها والمسموح لهم بالوصول إليها فقط بالنسبة للخدمات المُقدمة، سواءً في الموقع أو على السحابة.
(3)	ضمان عدم وجود ثغرات أمنية قد تُمكّن من الوصول غير المُصرّح به حتى داخل الأجزاء المُقيدة من النظام أو التطبيق.
(4)	تقييد الوصول بناءً على الحد الأدنى من الصلاحيات والأذونات اللازمة لأداء العمليات الروتينية ومسؤوليات دور العمل.
(5)	أن تكون الصلاحيات والأذونات الإضافية المطلوبة على الأقل: أ- مُبررة ومُتحقق منها بناءً على دور مُقدّم الطلب وكفاءاته. ب- مُراقبة بدقة لتجنب التأثير على الوصول غير المُصرّح به لأصل المعلومات أو المورد الذي تم الوصول إليه. ج- تمنح بشكل مؤقت - قدر الإمكان - بعد الحصول على تصريح من مالك أصل المعلومات أو المورد. د- موثقة ومسجلة.
(6)	منح الوصول المنطقي للجهات الخارجية، والموظفين المؤقتين، والمتعاقدين، والمُستعان بهم من جهات خارجية، والموردين، بشكل مؤقت، وبمدة زمنية محدودة لاحتياجات العمل الفعلية، مع تسجيله ومراقبته قدر الإمكان.
(7)	تقسيم الواجبات والأذونات الخاصة بالأنشطة والعمليات الحساسة والبالغة السرية وعمليات تكنولوجيا المعلومات بين شخصين مختلفين على الأقل من مجموعات مختلفة، لضمان عدم قيام الفرد الواحد بتنفيذ الأنشطة أو العمليات (ذات التحكم المزدوج)، وكذلك لضمان عدم القدرة على تجاوز التحكم المزدوج.
(8)	تمكين المصادقة متعددة العوامل في الأنظمة الحرجة والحساسة للأدوار المميزة المعينة بشكل دائم ومؤقت.
(9)	تحديد آلية للإبلاغ الفوري عن أي حقوق وصول استثنائية ممنوحة. وأن تضمن هذه الآلية التحقق من مطابقة الحقوق الممنوحة لقواعد التفويض المعتمدة مسبقاً.
(10)	مراجعة حقوق الوصول الممنوحة للأفراد بانتظام، وتعديلها بناءً على تغيير الأدوار، وإلغاؤها عند انتهاء صلاحيتها.

(11)	على مالكي أصول وموارد المعلومات مراجعة تصاريح حقوق الوصول المميزة بشكل دوري.
8.2.3.4	الوصول المنطقي (Logical Access)
8.2.3.4.1	الوصول إلى الشبكة (Network Access)
المبدأ	ضمان أن يكون السماح بالوصول إلى الشبكة وخدماتها قائماً على الهوية، ومتكاملاً مع نظام إدارة الهوية.
الهدف	تقييد التنقل عبر أجزاء الشبكة والوصول إلى خدماتها (مثل الإنترنت) من خلال التحكم في الوصول.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تكون للشبكة (نقاط الوصول، ومفاتيح شبكة الوصول، وبوابات VPN) مصادقة وتفويض لكل جهاز وفرد ، علي سبيل المثال لا الحصر(إعداد جزء من الشبكة).
(2)	أن تعتمد مصادقة الأجهزة على عمليات تشفير لا تعتمد على مفاتيح مشتركة مسبقاً.
(3)	تقييد التنقل عبر مكونات الشبكة والوصول إلى خدمات الشبكة علي سبيل المثال لا الحصر (المخدمات ، التطبيقات ، الانترنت) من خلال التحكم في الوصول على مستوى الشبكة (جدار حماية المخدمات وقواعد البيانات أو جدار حماية طبقة التطبيقات)، مما يعني رفض أي إجراء ما لم يُسمح به.
(4)	إجراء مراجعة دورية موثقة لقواعد الوصول إلى الشبكة مرتين سنوياً على الأقل.
8.2.3.4.2	الوصول الي التطبيقات (Applications Access)
المبدأ	التحكم في الوصول إلى المعلومات، وجميع مكونات نظام التطبيقات.
الهدف	ضمان عدم وجود ثغرات أمنية قد تُمكّن من الوصول غير المصرح به للتطبيقات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	التحكم في الوصول إلى المعلومات، وجميع مكونات نظام التطبيقات، ووظائفه، واستخراج المعلومات بناءً على دور العمل ومستوى امتيازات الفرد.
(2)	أن تتضمن التطبيقات رفضاً ضمنياً للإجراءات الإفتراضية.كما يجب على الجهة ضمان عدم وجود ثغرات أمنية قد تُمكّن من الوصول غير المصرح به حتى داخل الأجزاء المقيدة من النظام أو التطبيق.

(3)	تقييد جميع وصول الأفراد، باستثناء مسؤولي قواعد البيانات، إلى البيانات في نظام إدارة قواعد البيانات (DBMS)، من خلال أساليب برمجية.
(4)	أن يعتمد وصول التطبيقات إلى البيانات في نظام إدارة قواعد البيانات على هويات لا يستخدمها الأفراد أو الخدمات.
(5)	ضبط الحقوق والأذونات لخدمات التطبيقات على مستوى البنية التحتية ونظام التشغيل لتجنب منح حقوق وأذونات امتيازات دائمة.
(6)	أن تراعي سياسة إدارة كلمات المرور المعمول بها هويات التطبيقات والخدمات.
8.2.3.4.3	**صلاحيات الوصول الإداري (Administrative Access)**
المبدأ	إدارة مكونات البنية التحتية للشبكة ، والأمان للوصول إلى مكوناتها والأنظمة والتطبيقات.
الهدف	ضمان أن تعتمد الجهة نموذج للتحكم في الوصول إلى البنية التحتية والتقليل من خطر تصعيد الصلاحيات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	ضبط الوصول إلى مكونات البنية التحتية لتقليل من خطر تصعيد الصلاحيات من خلال تقييد ضوابط المسؤولين، ويسمح لهم بتسجيل الدخول والوصول إلى أصول المعلومات من خلال الآتي: أ- تقسيم مكونات وخدمات البنية التحتية لتكنولوجيا المعلومات بين مستويات أمان مختلفة. ب- يمكن لمسؤولي المستوى الأعلى التحكم في أصول المعلومات ذات المستوى الأدنى، ولكن لا يمكنهم تسجيل الدخول إليها، بينما لا يمكن لمسؤولي المستوى الأدنى التحكم في أصول المعلومات ذات المستوى الأعلى. ج- أن يشمل مستوى الأمان الأعلى خدمات إدارة الهوية، بينما يشمل مستوى الأمان الأدنى نقاط النهاية (الأجهزة الطرفية End Point).
(2)	عدم تفويض حقوق وأذونات إدارة تكنولوجيا المعلومات ذات الامتيازات العالية.
(3)	تشفير الوصول الإداري غير المرتبط بوحدة التحكم.
(4)	إدارة مكونات البنية التحتية للشبكة والأمان عبر واجهات إدارة مخصصة (مثل واجهة إدارة خارج النطاق) يتم الوصول إليها عبر شبكة مُتحكم بها علي سبيل المثال لا الحصر (Management VLAN).

(5)	فصل خدمات المصادقة للهويات المستخدمة لإدارة مكونات البنية التحتية للشبكة والأمان عن الهويات المستخدمة للوصول إلى مكونات البنية التحتية والأنظمة والتطبيقات الأخرى.
(6)	تنفيذ مهام الأعمال ذات الامتيازات، وعمليات تكنولوجيا المعلومات، والمهام الإدارية من خلال محطات عمل مادية أو افتراضية تقع في مناطق آمنة منطقية ومقيدة بالمهام المقصودة.
(7)	ألا تتمتع محطات العمل (Work Station) بإمكانية الوصول إلى نقاط يُحتمل أن تكون معرضة للتهديدات علي سبيل المثال لا الحصر (الإنترنت، وخدمات البريد الإلكتروني، والوصول عن بُعد) لتجنب هجمات الهوية، وتسريب البيانات ، والحفاظ على قنوات سرية.
(8)	على الجهة تطبيق تحكم دقيق في مكونات البنية التحتية والمخدمات ونسخ الحوسبة من خلال إنشاء مخدمات انتقالية مختلفة.
(9)	ربط المخدمات بمنطقة أمان واحدة (Security Zone) وتحديد موقعها، بحيث يمكن للمسؤولين الوصول اليها من خلال استخدام مخدمات الادارة (Management Servers).
(10)	تنفيذ المهام الإدارية باستخدام أدوات الإدارة (Management Tools) بدلاً من تسجيل الدخول التفاعلي أو عن بُعد (Interactive Or Remote Login) إلى المخدمات المُدارة ونسخ الحوسبة.
(11)	تسجيل جميع الإجراءات التي تتخذها الحسابات ذات الامتيازات (Privileged Accounts)على مكونات البنية التحتية والمخدمات، وكذلك الجلسات.
8.2.4	**حماية البيانات (Data Protection)**
8.2.4.1	**سرية البيانات (Data Confidentiality)**
المبدأ	حماية سرية البيانات والمعلومات السرية، بجميع أشكالها، أثناء التخزين والنقل.
الهدف	ضمان حماية البيانات بجميع أشكالها، أثناء التخزين والنقل.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	حماية سرية البيانات والمعلومات السرية، بجميع أشكالها، أثناء التخزين، من خلال مراعاة ما يلي على الأقل: أ- تطبيق آليات تشفير على المحتوى، والملفات، والتطبيقات، ونظم التشغيل، و/أو مستويات التخزين. ب- تقييد الوصول المادي والمنطقي للأفراد والأجهزة والسماح للمصرح لهم فقط. ج- الحد من نقاط التخزين والنسخ المتماثلة للبيانات والمعلومات السرية. د- حظر نقل البيانات والمعلومات السرية خارج ادوات(مواعين) الحفظ إلا بتصريح صريح من صاحب العمل بناءً على احتياجات العمل المحددة، مع إخفاء هوية البيانات وإخفائها قدر الإمكان، بالإضافة إلى تطبيق تدابير وإجراءات حماية تضمن عدم الإفصاح عن السرية خارج أدوات الحفظ.
(2)	حماية سرية البيانات والمعلومات السرية، بجميع أشكالها، أثناء النقل، من خلال مراعاة تطبيق آليات التشفير وتقييد الوصول على قناة النقل و/أو على مستويات المحتوى المرسل.
(3)	إخفاء هوية أي بيانات ومعلومات سرية تُرسل عبر قنوات نقل غير موثوقة وخارجة عن السيطرة.
(4)	أن يقتصر الإرسال الكامل للبيانات والمعلومات السرية عبر هذه القنوات على كلمات مرور مؤقتة وكلمات مرور للاستخدام مرة واحدة ذات صلاحية قصيرة.
(5)	استخدام طرود مختومة مقاومة للعبث لنقل البيانات والمعلومات السرية عبر وسائط النقل المادية (البريد).
8.2.4.2	**سلامة البيانات Data Integrity**
المبدأ	ضمان عمليات التحقق من السلامة واكتشاف أي تغييرات أو تعديلات غير متوقعة.
الهدف	ضمان سلامة المعلومات والبيانات من حدوث اي تغييرات في المحتوي.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	حماية سلامة المعلومات والبيانات في حالة السكون (At Rest)، مع مراعاة ما يلي على الأقل: أ- بيانات ومعلومات المستخدم السرية.

	ب- ملفات نظام التشغيل وقطاعات التمهيد (Boot Sectors). ج- تشـــغيل الملفات التنفيذية للبرامج والتطبيقات والملفات الثابتة (لتعديل المحتوى وإضافة أو حذف ملفات غير متوقعة). د- سجلات قواعد البيانات (وليس ملفات البيانات أو السجلات). يجب إجراء فحص مرجعي شامل لجميع السجلات. هـ- سجلات الأنظمة والتطبيقات الحالية ومسارات التدقيق. و- أن تعتمد استمرارية وانتظام عمليات فحص السلامة على تقييم المخاطر، بالإضافة إلى تصنيف أصول المعلومات.
(2)	التحقق من مصدر وسلامة البرامج وتحديثات الأمان والتصحيحات والتحقق من صحتها قبل التثبيت أو التطبيق.
(3)	مراعاة حماية ســرية البيانات والمعلومات بفحص ســلامة المعلومات أو البيانات في حالة الســكون (المخزنة) عن طريق التحقق من مجاميع التحقق (Checksum) والتوقيعات الرقمية التي يوفرها المصدر عند الاكتمال.
(4)	تهيئة أصول المعلومات الحرجة والحساسة لتشغيل وتنفيذ البرامج الموثوقة فقط. ويمكن تحقيق ذلك باستخدام تقنيات القائمة البيضاء (Wight list).
(5)	أن تضمن عمليات التحقق من السلامة اكتشاف أي تغييرات في الملفات أو إضافات غير متوقعة وتسجيلها أو إصدار تنبيهات بشأنها. يجب اعتبار التنبيهات بيانات جنائية.
(6)	أن تضــمن الأنظمة والتطبيقات ســلامة البيانات والمعلومات أثناء النقل، وأن تراعي على الأقل ما يلي: أ- الإعتمـاد على التوقيع الرقمي بـدلاً من مجموعـات التحقق للتحقق من سـلامة البيانات، بالإضـافة إلى تطبيق ضـوابط السـرية على مسـتوى قناة النقل و/أو المحتوى. ب- وضــع ختم زمني على الرســائل المرســلة و/أو تضــمين رمز خاص لتجنب هجمات إعادة التشغيل. ج- تسـلسـل الرسـائل المرسـلة بطريقة تُمكّن من اكتشـاف الإرسـالات ذات التسلسل غير الصحيح (أي الإرسالات غير المتوافقة مع الترتيب). د- الإشارة إلى تبعيات الرسائل المرسلة. هـ- اكتشاف التكرارات ومعالجتها.

	و- تأكيد استلام الرسائل المرسلة لضمان إثبات التسليم.
(7)	أن تعتمد طبقة الشبكة لقناة النقل على بروتوكول (TCP Protocol)، ويجب أن تستخدم الأجهزة ذاكرة الوصول العشوائي التي تقوم بتصحيح تلف البيانات الداخلية (ECC RAM).
(8)	يمكن أن تكون عملية التحقق من السلامة عملية يدوية، مدمجة في المنتج، أو يمكن أن تعتمد على أداة تابعة لجهة خارجية .
8.2.4.3	**مصادقة البيانات (Data Authentication)**
المبدأ	تطبيق آليات لضمان مصادقة البيانات المُستلَمة عبر التطبيقات والأنظمة وذلك بالنسبة للبيانات والمعاملات المؤثرة على الأعمال.
الهدف	ضمان مصادقة البيانات المُستلَمة وحمايتها من وقوع هجمات الوسيط.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	حماية الأسرار المشتركة (Shared Secrets) بشكل آمن لمنع الوصول غير المصرح به والإفصاح عنها في حالة استخدام آلية تعتمد على التشفير المتماثل (Symmetric Cryptographic).
(2)	حماية المفاتيح الخاصة (Private Keys) بشكل آمن لمنع الوصول غير المصرح به والإفصاح عنها في حالة استخدام آلية تعتمد على التشفير غير المتماثل (Asymmetric Cryptographic) علي سبيل المثال لا الحصر (التوقيع الرقمي والمصادقة القائمة على الشهادات)،
(3)	أن تكون المفاتيح العامة (Public Keys)على شكل شهادات رقمية(X.509v3) صادرة من سلطة تصديق موثوقة بالنسبة للجهات الخارجية والخدمات خارج نطاق الجهة.
8.2.4.4	**عدم الإنكار (Non-Repudiation)**
المبدأ	النظر في تطبيق نظم تضمن تسليم المُستلمين المعاملات دون انكار.
الهدف	تثبيت الآليات المُعتمدة لضمان عدم التنصل في اجراء المعاملات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تطبيق آليات تضمن اجراء المعاملات بإثبات التسليم، بالنسبة للمعاملات المؤثرة على الأعمال.

(2)	تسليم المُستلمين بإثبات هويتهم، بحيث لا يستطيع أي منهما لاحقاً إنكار معالجة المعلومات.
8.2.4.5	**خصوصية البيانات (Data Privacy)**
المبدأ	وضع سياسة واجراءات خصوصية بيانات، وصيانتها، وتطبيقها، وتعميمها.
الهدف	ضمان معالجة البيانات الشخصية بشكل قانوني وعادل وشفاف تجاه مالك البيانات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تتناول السياسة والإجراءات ما يلي: أ. معالجة البيانات الشخصية بشكل قانوني وعادل . ب. أن تستند قانونية جمع ومعالجة البيانات الشخصية إلى: i. الحصول على موافقة واضحة وصريحة لا يمكن إنكارها من مالك البيانات. ii. الإلتزامات التعاقدية عندما يكون مالك البيانات طرفًا في العقد، أو لاتخاذ خطوات محددة يطلبها مالك البيانات قبل إبرام العقد. iii. عندما تكون الجهة خاضعةً للالتزامات القانونية التاليه: a. وظيفة رسمية أو مهمة في المصلحة العامة، وأن يكون للوظيفة أو المهمة أساس واضح في القانون أو اللوائح. b. المصالح المشروعة التي تسعى إليها الجهة أو طرف ثالث ما لم تكن هذه المصالح غير متجاوزة لمصالح مالك البيانات أو حقوقه الأساسية التي تتطلب حماية البيانات الشخصية. ج. أن يكون لمالك البيانات القدرة على تحديد انتهاء صلاحية الموافقة، بالإضافة إلى الحق في سحبها في أي وقت. د. تُجمع البيانات الشخصية حسب الحاجة لأغراض محددة مسبقًا وصريحة ومشروعة. أو تكون البيانات ذات صلة ومقتصرة على هذه الأغراض فقط. هـ. تُخزن البيانات الشخصية وتُعالج بطريقة تُحدد هوية مالك البيانات لفترة لا تتجاوز المدة اللازمة للأغراض المحددة مسبقاً. و. أن تستوفي أرشفة البيانات الشخصية المتطلبات القانونية والتنظيمية.	

	ز. أن يتمتع مالك البيانات بالحق في محو بياناته الشخصية بعد سحب الموافقة، مالم توجد متطلبات قانونية أو تنظيمية. ح. ضمان أمن البيانات (السرية والنزاهة) أثناء النقل والمعالجة والتخزين. ط. ضمان جودة البيانات من خلال الحفاظ على عمليات تنظيف البيانات وتحديثها لتصحيح أي بيانات غير دقيقة.
(2)	إبلاغ السياسة والاجراءات للطرف الثالث ومقدمي الخدمات والموردون، وضمان إلتزام هذه الأطراف بالسياسة.
8.2.5	**حماية المعلومات (Information Protection)**
8.2.5.1	**إدارة التهيئة (Configuration Management)**
المبدأ	وضع وتطوير سياسات وإجراءات إدارة التهيئة وصيانتها وتنفيذها والتواصل بشأنها لضمان الحفاظ على عناصر التهيئة.
الهدف	ضمان أن تأخذ السياسات والإجراءات المحددة في الاعتبار التحكم في إدارة التهيئة وتغييرها ومراقبتها.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد كل جزء من كل نظام (Configuration Items) الذي يُعد هدفاً منفصلاً لعمليات إدارة التهيئة علي سبيل المثال لا الحصر (الأجهزة، المشرف الافتراضي، نظام التشغيل، برامج التطبيقات، برامج الأمان، أجهزة الشبكة، الوثائق). كما يجب تحقيق هذه الخطوة من خلال عملية جرد الأصول.
(2)	تحديد التهيئة الأساسية (Baseline Configuration) من خلال تحديد مجموعة من المواصفات لكل نظام ولكل عنصر تهيئة داخله.
(3)	مراجعة التهيئة الأساسية لفترة زمنية محددة بصورة رسمية والموافقة عليه.
(4)	معالجة جميع التغييرات من خلال عملية إدارة التغيير.
(5)	أن تتناول التهيئة الأساسية على الأقل ما يلي: أ- إعدادات التهيئة (Configuration Management). ب- أحمال البرامج ومستويات التصحيح (Software Upload & Patches). ج- كيفية ترتيب نظام المعلومات مادياً أو منطقياً.

	د- كيفية تنفيذ ضوابط الأمان المختلفة. هـ- إجراء التوثيق.
(6)	تحديد عملية مراقبة لتقييم مستوى الإلتزام للتهيئة الأساسية المُحدده.
(7)	نشر آليات الإبلاغ عن حالة تكوين العناصر الخاضعة لإدارة التهيئة.
8.2.5.2	**إدارة التغيير (Change Management)**
المبدأ	وجود عملية مُحكمة لمراقبة جميع التغييرات التي تطرأ على أصول المعلومات.
الهدف	وضع واعتماد وتنفيذ عملية متكاملة لإدارة التغيير، بما يضمن التحكم في جميع التغييرات التي تطرأ على أصول المعلومات مع متابعة الإلتزام والقياس والتقييم بشكل دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أ- وضع إجراءات واضحة للتعامل مع الأنواع التالية من التغييرات: i. التغييرات القياسية: المُصرّح بها مسبقاً، وفقاً لإجراءات مُحددة مسبقاً. ii. التغييرات الطارئة: التي تتطلب التنفيذ الفوري. iii. التغييرات العادية. ب- تعيين مدير للتغيير يتولى مسؤولية الإشراف الكامل على عملية إدارة التغيير، بما في ذلك: i. منح الموافقة النهائية على فئات التغيير المحددة. ii. تحديد الأولويات. iii. تتبع ومراقبة حالة التغييرات. ج- تشكيل لجنة استشارية للتغيير تتولى مسؤولية تقدير الأثر، وتحديد الموارد المطلوبة، والموافقة النهائية على قرارات مدير التغيير أو مراجعتها وتأكيدها. على أن تضم في عضويتها على الأقل: i. مدير إدارة الأمن السيبراني. ii. مدير إدارة تقنية المعلومات. iii. مدير إدارة العمليات. iv. مدير إدارة علاقات العملاء.

(2)	أن يقوم مدير التغيير بتصنيف التغييرات العادية إلى ثلاث فئات على الأقل: رئيسية، هامة، وطفيفة، بناءً على درجة التعقيد ومستوى المخاطرة، مع تحديد صلاحيات اعتماد مختلفة لكل فئة وفقاً للآتي: أ- تتم الموافقة المبدئية على طلب التغيير من قبل إدارة العمليات، ثم من مدير إدارة الأمن السيبراني، قبل تقديمه إلى مدير التغيير. ب- يتم تقديم التغييرات الرئيسية والهامة عبر مدير التغيير إلى اللجنة الاستشارية للحصول على الموافقة النهائية، بعد تحديد المخاطر وتدابير التخفيف المناسبة. ج- تتم الموافقة النهائية على التغييرات الطفيفة من قبل مدير التغيير، بعد مراجعتها وتأكيدها من قبل اللجنة الاستشارية لتخصيص الموارد اللازمة وجدولة التغيير. د- في حالة التغييرات الطارئة، يمكن لمدير التغيير التواصل مباشرة مع الإدارة العليا، لجنة الأمن السيبراني، أو مجلس الإدارة لاعتمادها.
(3)	تنفيذ خطط اختبار وخطط تراجع لكل تغيير معتمد. على أن يتم تنفيذ الاختبارات في بيئة مخصصة لذلك، وتشمل على الأقل: أ- اختبارات القبول الوظيفي، قبول المستخدم، التكامل، والضغط. ب- اختبارات الأمان، والتي تتضمن: i. إدارة الهوية. ii. معالجة الاستثناءات. iii. وظائف التسجيل والتدقيق. iv. مراجعة الكود الثابت قدر الأمكان. v. تحليل الكود الديناميكي عبر فحص الثغرات الأمنية واختبارات الاختراق.
(4)	القيام بالتوثيق الكامل، إجراء الاختبارات، والحصول على الموافقات اللازمة قبل تنفيذ التغيير في بيئة الإنتاج.
(5)	تسجيل ومراقبة نتائج تنفيذ التغيير.
(6)	إجراء مراجعة ما بعد التنفيذ لضوابط الأمن السيبراني، على سبيل المثال لا الحصر (التهيئة، جرد الأصول، وغيرها).

(7)	مراقبة الإلتزام بسياسات وإجراءات إدارة التغيير.
8.2.5.3	إدارة التصحيحات ومعالجة الثغرات (Patch and Vulnerability Management)
المبدأ	تحديد الضوابط التصحيحية ومعالجة الثغرات بحيث لا تؤثر سلباً على التطبيقات وسير الأعمال.
الهدف	ضمان تنزيل التصحيحات الفعالة ومعالجة ثغرات جميع عناصر التهيئة المحددة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن تشمل الأصول المحددة في سياسة وإجراءات إدارة الثغرات جميع عناصر التهيئة التالية كحد ادنى: أ- أنظمة التشغيل ،برنامج (Hypervisor)، البرامج الثابتة، وبرامج تشغيل التطبيقات. ب- تطبيقات المخدمات، تطبيقات سطح المكتب، وتطبيقات الأجهزة المحمولة، بالإضافة إلى البرامج الوسيطة (APIs) وأنظمة إدارة قواعد البيانات. ج- أجهزة الشبكة.
(2)	أن تشمل منهجيات تحديد الثغرات ما يلي كحد أدنى: أ- عملية دورية لربط وإيجاد التطابقات بين معدات (CPE) المُخزّنة، وثغرات (CVE) المنشورة، وأنظمة (CVSS) ذات الصلة. ب- تلقي الإشعارات من الموردين ،والشركاء الخارجيين،وفرق الإستجابة لطوارئ الحاسب الآلي (إن وجدت) عبر قنوات موثوقة مثل رسائل البريد الإلكتروني، الموردين أو مقدمي الخدمات، وبرامج إدارة التصحيحات. ج- نتائج عمليات فحص الثغرات واختبار الاختراق، بالإضافة إلى ضوابط الأمن السيبراني الأخرى.
(3)	تحديد الإجراءات التصحيحية الممكنة بناءً على توصيات (CVE) والموردين.
(4)	إجراء عملية تقييم للمخاطر الناتجة عن الأثر السلبي للإجراءات التصحيحية على التطبيقات وسير الأعمال .
(5)	أن تمر المعالجة بعملية إدارة التغيير المعتمدة.

(6)	أن يُراعى في تصنيف الثغرات الأمنية وتحديد أولوياتها ما يلي: أ- قيمة درجة الثغرة بناءاً علي نظام تقييم الثغرات المعروف (CVSS)، وما إذا كانت الثغرة قد استُغلت سابقاً. ب- نوع وموقع الأصل المعرض للخطر، علي سبيل المثال لا الحصر (الإنترنت، التعامل مع الجمهور، التواصل مع شبكات، جهات غير موثوقة، نظام إدارة قواعد البيانات). ج- وزن الأصل المعرض للخطر بناءً على خطورته وحساسيته.
8.2.5.4	**إدارة أمن التطبيقات (Applications Security Management)**
المبدأ	تحديد معايير الأمن السيبراني لأنظمة التطبيقات واعتمادها وتطبيقها.
الهدف	ضمان وضع وتوثيق ضوابط الأمن السيبراني الكافية، وتنفيذها لجميع التطبيقات، ومراقبة الإلتزام وتقييم فعاليتها بشكل دوري داخل الجهة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	قياس فعالية ضوابط الأمن السيبراني للتطبيقات وتقييمها دورياً.
(2)	أن يتبع تطوير التطبيقات منهجية دورة حياة تطوير النظام الآمنة (SDLC) المعتمدة.
(3)	أن يشمل معيار أمن التطبيقات ما يلي: أ- معايير الترميز الآمن. ب- ضوابط الأمن السيبراني المُطبقة علي سبيل المثال لا الحصر (معلمات التهيئة، أحداث المراقبة والاحتفاظ ، وإدارة الهوية والوصول). ج- فصل المهام داخل التطبيق (مع دعم مصفوفة تفويض موثقة). د- حماية البيانات بما يتوافق مع نظام التصنيف المتفق عليه، بما في ذلك خصوصية بيانات العميل، وتجنب الوصول غير المصرح به وتسريب البيانات غير المقصود. هـ- إدارة الثغرات الأمنية والتصحيحات. و- إجراءات النسخ الاحتياطي والاسترداد. ز- مراجعة دورية للإلتزام بالأمن السيبراني.

8.2.5.5	إدارة الاحتفاظ والإهلاك (Retention and disposal Management)
المبدأ	وضع وتطوير وتنفيذ سياسة وإجراءات الاحتفاظ بالمعلومات وإهلاكها بشكل آمن لضمان الحماية من التسرب والوصول غير المصرح به.
الهدف	ضمان حفظ وحماية المعلومات من التسرب والوصول غير المصرح به، وإهلاكها بشكل آمن.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد سياسة الاحتفاظ بأصول المعلومات وأرشفتها وفقا للمتطلبات القانونية والتنظيمية، بالإضافة إلى احتياجات العمل.
(2)	ضمان عدم تدهور وسائط التخزين خلال فترة التخزين المطلوبة.
(3)	التخلص من أصول المعلومات وإهلاكها عند عدم الحاجة إليها وفقاً للمتطلبات القانونية والتنظيمية، وذلك باستخدام تقنيات ووسائل محو دائم تجعل استعادة البيانات والمعلومات السرية مستحيلة.
(4)	ضمان تطبيق سياسة الاحتفاظ بالمعلومات وإهلاكها عند معالجة البيانات و/أو تخزينها من قبل أطراف ثالثة ومقدمي خدمات وموردين وفقًا لسياسة تصنيف البيانات.
(5)	ضمان التزام مقدمي خدمات السحابة بالسياسة عند عدم الحاجة إلى البيانات والمعلومات أو عند نقلها للخارج (أي الخروج).
(6)	توضيح التزام مقدم خدمة السحابة بسياسة الاحتفاظ بالبيانات من خلال العقد الملزم.
8.3	أمن البنية التحتية والشبكات (Infrastructure and Network Security)
8.3.1	أمن البنية التحتية (Infrastructure Security)
المبدأ	تحديد وتطوير معايير وضوابط الأمن السيبراني لمكونات البنية التحتية واعتمادها وتطبيقها.
الهدف	ضمان عملية تنفيذ وتوثيق جميع ضوابط الأمن السيبراني داخل البنية التحتية ومراقبة الإلتزام وتقييم فعاليتها بشكل دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	قياس فعالية ضوابط الأمن السيبراني للبنية التحتية وتقييمها دورياً.

(2)	أن تغطي معايير أمن البنية التحتية جميع أنواع البنية التحتية المتاحة في مراكز البيانات الرئيسية، ومواقع التعافي من الكوارث، والمساحات المكتبية.
(3)	أن تغطي معايير أمن البنية التحتية جميع الأنواع والمكونات علي سبيل المثال لا الحصر (أنظمة التشغيل، والمخدمات ، والأجهزة الافتراضية، وجدران الحماية، وأجهزة الشبكة، وأنظمة كشف التسلل (IDS)، وأنظمة منع التسلل (IPS)، والشبكات اللاسلكية، وبوابات البريد الإلكتروني، والاتصالات الخارجية، وقواعد البيانات، ومشاركات الملفات، ومحطات العمل، وأجهزة الكمبيوتر المحمولة، والأجهزة اللوحية، والأجهزة المحمولة).
(4)	أن يشمل معيار أمن البنية التحتية ما يلي: أ- ضوابط الأمن السيبراني المُطبقة علي سبيل المثال لا الحصر معلمات التهيئة (Parameters Configurations)، وأحداث المراقبة والاحتفاظ والوصول إلى النظام والبيانات، ومنع تسرب البيانات [DLP]، وإدارة الهوية والوصول، والوصول عن بُعد. ب- فصل المهام ضمن مكون البنية التحتية (مدعوماً بمصفوفة تفويض موثقة). ج- حماية البيانات بما يتماشى مع نظام التصنيف المتفق عليه بما في ذلك خصوصية بيانات العميل، وتجنب الوصول غير المصرح به وتسريب البيانات غير المقصود. د- استخدام برامج معتمدة وبروتوكولات آمنة. هـ- تجزئة الشبكات إلى إجزاء منفصلة عبر استخدام الفصل (المادي / المنطقي VLAN, Zone). و- الحماية من البرامج الخبيثة والأكواد الضارة والفيروسات . ز- تطبيق القائمة البيضاء للتطبيقات والحماية من التهديدات المتقدمة المستمرة. ح- إدارة الثغرات الأمنية والتصحيحات. ط- الحماية من (DDOS) ويجب أن يشمل ذلك: i. مراقبة على مدار الساعة طوال أيام الأسبوع من خلال تشغيل الانظمة الخاصة بالمراقبة الحديثة.

	ii. اختبار تنظيف هجمات حجب الخدمة الموزعة (DDOS) مرتين سنوياً على الأقل. iii. تطبيق خدمات منع حجب الخدمة الموزعة (DDOS) في مراكز البيانات الرئيسية، بالإضافة إلى مواقع التعافي من الكوارث. ي- إجراءات النسخ الاحتياطي والاسترداد. ك- المراقبة والإلتزام بشكل دوري .
8.3.2	**تقوية النظام والتطبيق (System and Application Hardening)**
المبدأ	وضع وتنفيذ إجراءات تقوية النظام والتطبيق لضمان التهيئة الآمنة.
الهدف	حماية الأنظمة والتطبيقات ومنع الوصول إلى المخدمات التي يُحتمل اعتبارها نقاط دخول وخروج للتهديدات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تقوية جميع الأنظمة والتطبيقات وفقاً لإرشادات الأمان الخاصة بالموردين ومعايير الصناعة، وتنفيذ متطلبات التهيئة الخاصة بالتطبيق للحفاظ على حالة تشغيلية سليمة.
(2)	على مسؤولي النظام مراعاة تنفيذ الخطوات التالية على الأقل: أ- أن تكون المخدمات مخصصة لغرض واحد، علي سبيل المثال لا الحصر(تجنب تشغيل كلاً من خدمات الويب وخدمات (DNS) على نفس المخدم إذا كان مخدم فعلي أو افتراضي. ب- ازالة جميع المكونات غير الضرورية، أو تعطّيل تلك التي لا يمكن إزالتها، وتثبيت الحد الأدنى من تكوين نظام التشغيل، ثم إضافة المكونات التاليه حسب الحاجة على سبيل المثال لا الحصر: i. ميزات النظام ووحدات النظام الفرعي (System Features And Subsystem Modules) ii. التطبيقات (Application)، وحدات التطبيقات (Modules)، حزم التطبيقات(Application Packages)، والإضافات (Add-Ons). iii. المخدمات (Services). iv. برامج التشغيل والبرامج الثابتة (Drivers and Firmware). v. البرامج النصية (Scripts).

	vi. بروتوكولات الشبكة (IPv4، وIPv6، وSMB، وNFS، وTelnet، وغيرها.) ج- تهيئة الأنظمة وضبطها لتشغيل التطبيقات والعمليات والخدمات باستخدام بيانات معتمدة وحسابات مقيدة (Restricted Credentials And Accounts)، حيث يُمنح الوصول إلى موارد النظام حسب الحاجة. د- إدراج التطبيقات الموثوقة المحددة مسبقًا في القائمة البيضاء فقط لتشغيلها على النظام. هـ- إعادة تسمية حسابات الإدارة الافتراضية (Default Administrative Accounts)قدر الإمكان، وتغيير جميع كلمات المرور الافتراضية للنظام والتطبيقات، وإزالة أو تعطيل حسابات المستخدمين غير الضرورية. و- ضبط خيارات القفل التلقائي لأجهزة الحاسوب بعد 5 دقايق من عدم النشاط. ز- تغيير جميع سلاسل مجتمع ومفاتيح التشفير الافتراضية (Default SNMP Community Strings). ح- تقييد المنافذ المادية مثل (USB).
(3)	توثيق وتبرير أي انحرافات عن معايير تهيئة التحصين المُختارة ، والضوابط المُطبقة كجزء من عملية إدارة التهيئة.
(4)	إجراء عملية مراجعة لإعدادات التهيئة وتوثيقها بشكل دوري - مرتين سنويًا على الأقل - وعند كل حالة تغيير.
8.3.3	**الوصول عن بعد (Remote Access)**
المبدأ	الحفاظ على سياسة وإجراءات وصول المستخدمين عن بُعد، وتطبيقها، والتواصل بشأنها.
الهدف	أن يمر الوصول عن بُعد إلى أصول المعلومات ومواردها عبر قنوات مؤمنة من البداية إلى النهاية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن يستند منح أذونات الوصول عن بُعد والفترات الزمنية إلى احتياجات العمل.
(2)	استخدام قنوات مؤمنة من البداية إلى النهاية علي سبيل المثال لا الحصر (TLS أو IPSec) مُنشأة عبر الشبكة العامة (مثل الإنترنت).

(3)	إنهاء القنوات المُنشأة على الشبكة عند جزء مُتحكم به جيدًا ومُخصصة لأغراض مُحددة تقع عند الحدود قبل تمرير الحزم الواردة إلى الشبكة الداخلية.
(4)	تأمين قنوات الوصول عن بُعد باستخدام آليات ومعايير تشفير قوية.
(5)	ضرورة العمل فقط على الأجهزة الخاصة بالجهة قدر الإمكان، وتطبيق آليات لمصادقة الجهاز (مثلاً، بناءً على الشهادة الرقمية).
(6)	مراعاة مبدأ بنية الثقة الصفرية (Zero Trust Architecture) للأجهزة الخاصه بها عند نقلها خارج شبكتها للوصول عن بُعد، ومبدأ إحضار الأجهزة الشخصية (BYOD) عند استخدامها للوصول عن بُعد.
(7)	تطبيق آليات مصادقة ثنائية العوامل على الأقل لمصادقة المستخدمين قبل الوصول إلى أصول وموارد المعلومات الداخلية (أي عند نقطة نهاية القناة).
(8)	فصل خدمات المصادقة للهويات المستخدمة لمصادقة المستخدمين عن بُعد عند نقاط نهاية القناة، عن الهويات المستخدمة للوصول إلى أصول وموارد المعلومات الأخرى داخلياً.
(9)	حظر نسخ ونقل وتخزين البيانات والمعلومات السرية على محركات الأقراص الصلبة المحلية (Hard Drives Local) والوسائط الإلكترونية القابلة للإزالة، إلا إذا تم التصريح بذلك صراحةً لحاجة عمل محددة.
(10)	ضمان تحديث وتصحيح الأجهزة المتصلة عن بعد .
(11)	عزل الأجهزة غير المحدثة ومعالجتها قبل الوصول إلى أصول وموارد المعلومات الداخلية.
(12)	أن تضمن التقنية المستخدمة فصل الجلسات غير النشطة، وتدمير جميع مفاتيح التشفير المتفق عليها بعد إنهاء الجلسة أو فصلها.
(13)	تقييد وصول المستخدم غير المُتحكم فيه إلى الإنترنت أثناء جلسة الوصول عن بُعد.
(14)	تثبيت جدار الحماية الشخصي (Personal Firewall) أو ما يعادله، وتهيئته بشكل صحيح، وتشغيله دائماً على الأجهزة المتصلة عن بعد.
(15)	توعية المستخدمين النهائيين بتجنب توصيل الأجهزة المتصلة عن بعد بشبكات لاسلكية عامة، وعدم تركها دون مراقبة في الأماكن العامة.
(16)	وضع حدود للإجتماعات التي تُعقد عبر الإنترنت للحفاظ على خصوصية المناقشات.
(17)	منح موظفي الدعم الخارجي إمكانية الوصول عن بُعد بشكل مؤقت، وبمدة زمنية محددة بحسب احتياجات العمل الفعلية،وتسجيل جلسات الوصول عن بُعد ومراقبتها قدر الإمكان.

(18)	إجراء مراجعة دورية - مرتين سنويًا على الأقل - وتحديثها باستمرار، لإعدادات التهيئة وتوثيقها.
(19)	تسجيل أنشطة الوصول عن بُعد ومراقبتها.
8.3.4	**التشفير (Cryptography)**
المبدأ	تحديد استخدام الحلول التشفيرية داخل جميع مكونات البنية التحتية والموافقة عليها وتنفيذها.
الهدف	ضمان تطبيق ضوابط التشفير علي جميع البيانات والمراسلات بغرض حمايتها والحفاظ على الخصوصية وسلامة المعاملات.
الضوابط	
في سبيل تطبيق نظام تشفير قوي ومتطور يجب على الجهة الإلتزام بالآتي:	
(1)	تشفير جميع البيانات المصنفة على أنها سرية أو سرية للغاية علي سبيل المثال لا الحصر (بيانات العملاء الشخصية، بيانات البطاقات، كلمات المرور، التسجيلات الحساسة) سواء أثناء تخزينها (Data at Rest) أو أثناء نقلها عبر الشبكات (Data in Transit).
(2)	استخدام بروتوكولات تشفير قوية بإصدارات حديثة وآمنة مثل (TLS/SSL) لحماية البيانات المنقولة بين الأنظمة الداخلية أو بين الجهة وعملائه أو بين الجهة وأطراف ثالثة.
(3)	تطبيق تقنيات تشفير قوية على الأقل (AES-256) على البيانات الحساسة المخزنة في قواعد البيانات، الملفات، المخدمات، وأجهزة التخزين.
(4)	تشفير أجهزة الهواتف المحمولة والأجهزة المحمولة (Laptops) التي تحتوي على بيانات حساسة.
(5)	إدارة مفاتيح التشفير بصورة صارمة وفق الآتي: أ- فصل أماكن تخزين مفاتيح التشفير عن أماكن تخزين البيانات المشفرة. ب- حماية مفاتيح التشفير باستخدام أجهزة متخصصة وآمنة للتخزين Security Modules (HSMs - Hardware كلما أمكن ذلك. ج- وجود سياسات صارمة لتوليد المفاتيح، توزيعها، تخزينها، تدويرها (استبدالها دورياً)، واسترجاعها، وحذفها بشكل آمن. د- تجنب استخدام نفس المفاتيح في بيئات التطوير والاختبار والإنتاج. هـ- أتمتة أجزاء دورة حياة المفاتيح قدر الإمكان. و- تقسيم المفاتيح عند التخزين والتوزيع إلى أجزاء متعددة عند الانتهاء .

	ز- ضمان فصل المهام في عمليات إدارة المفاتيح قدر الإمكان.
(6)	استخدام خوارزميات التشفير قوية كما يلي: أ- استخدام خوارزميات تشفير قوية وموثوقة ومعتمدة عالمياً وعدم استخدام خوارزميات ضعيفة أو قديمة تم كسرها (MD5 ، SHA-1، DES). ب- يُفضل استخدام خوارزميات معتمدة من هيئات معروفة علي سبيل المثال لا الحصر (NIST).
(7)	تشفير متطور للتطبيقات المالية ،خاصة التطبيقات الموجهة للعملاء علي سبيل المثال لاالحصر(الخدمات المصرفية عبر الإنترنت وتطبيقات الهواتف المحمولة)، بالاضافة إلى استخدام تقنيات التشفير لحماية جلسات العملاء وبياناتهم.
8.3.5	**المراقبة والكشف المنطقي (Logical Monitoring and Detection)**
المبدأ	تطبيق آليات كشف لمراقبة بنية الشبكة وتدفقاتها واستخدامها، ورصد أي انحرافات عن المسارات.
الهدف	ضمان دقة عملية المراقبة لجميع المعلومات التي تمر عبر شبكة الجهة.
الضوابط	
يجب علي الجهة اجراء المراقبة الدقيقة وفق الآتي:	
(1)	الكشف عن الاستخدام والاستهلاك غير المعتاد لموارد الشبكة وعرض النطاق الترددي (تحميل عرض النطاق الترددي للإنترنت).
(2)	أن تكون عملية المراقبة دقيقة (لكل مستخدم ، مصدر وجلسة شبكة).
(3)	جمع معلومات تدفق الشبكة. وبناء خط أساس لتدفقات الشبكة وصيانتها.
(4)	إطلاق تنبيهات عند حدوث اي انحرافات في تدفقات حزم الشبكة (Deviations of The Flows Should Trigger Alerts).
(5)	التقاط حزم الشبكة (Capture Network Packets) بطريقة تُمكّن من إعادة بناء جلسات الشبكة. وتحديد المقاطع المحددة وفترة الاحتفاظ بالحزم الملتقطة بناءً على عملية تقييم المخاطر.
(6)	الكشف عن نقاط الوصول غير الموثوقة (Detect Rogue Access Points) وحركة مرور الشبكة غير الموثوقة (Rogue Network Traffic). كما يجب الكشف عن التغييرات في طبقات الحماية او الامان.

(7)	مراقبة نشـــاط المســـتخدم والخدمة على مســـتوى الشـــبكة ونظام التشـــغيل والخدمة والتطبيق.
(8)	أن تشمل المراقبة والتسجيل على الأقل ما يلي: أ- محاولات تسجيل الدخول الفاشلة وتكرار إغلاق الحسابات. ب- محاولات تسجيل الدخول التفاعلية لحسابات الخدمة. ج- محاولات تسجيل الدخول باستخدام حسابات ذات امتيازات وحسابات افتراضية للمورد. د- محاولات تسجيل الدخول باستخدام حسابات معطلة أو منتهية الصلاحية. هـ- محاولات تسجيل الدخول باستخدام حسابات وهمية. و- تكرار محاولات تسجيل الدخول حسب اليوم، والوقت (مثلاً: خارج ساعات العمل)، والموقع (مثلاً: تسجيل الدخول من موقع لم يُستخدم من قبل)، والجهاز (مثلاً: نفس الحساب من مصادر متعددة أو حسابات متعددة من نفس المصدر). ز- أنواع محاولات تسجيل الدخول (مثلاً: تفاعلية، كخدمة، إلخ.) ح- الوقت منذ آخر تسجيل دخول.
(9)	مراقبة خدمات المصادقة وعمليات تعديل المستخدمين. بحيث تشمل المراقبة والتسجيل ما يلي: أ- التنبيه عند إنشـــاء بيانات الاعتماد ثم حذفها خلال فترات قصـــيرة، وعند إنشاء اوحذف مجموعة كبيرة من المستخدمين خلال فترات قصيرة. ب- التنبيه عند تغيير كلمات المرور بشكل متكرر خلال فترة قصيرة. ج- تغييرات عضوية المجموعة ذات الامتيازات. د- تكون المراقبة والتسجيل على مستويات: i. الشـــبكة: مثل الوصـــول إلى قاعدة رفض الوصـــول الصـــريحة أو الضـــمنية، أو فشـــل تســـجيل الدخول إلى نظام التحكم في قبول الشـبكة، أو فشـل تسـجيل الدخول إلى نقطة نهاية الوصـول عن بُعد وغيرها. ii. نظام التشغيل، والبرامج الثابتة، والتطبيقات، وموارد المعلومات.

8.3.5.1	كشف النشاط الضار (Detecting Malicious Activity)
المبدأ	تطبيق آليات الكشف لرصد الأنشطة الضارة.
الهدف	تطبيق حلول مكافحة الفيروسات والبرامج الضارة.
الضوابط	
يجب علي الجهة مكافحة البرامج الضارة وفق الآتي:	
(1)	تطبيق حلول لمنع التطفل قائمة على التوقيع والسلوك على مستوى الشبكة والمضيف (Host).
(2)	تطبيق حلول تحليل مكافحة الفيروسات والبرامج الضارة، قائمة على الشبكة والمضيف، وقائمة على التوقيع والسلوك.
(3)	تقديم خدمات تخفيف هجمات حجب الخدمة (DoS) وهجمات حجب الخدمة الموزعة (DDoS) (الحجمية وغير الحجمية) لحماية الخدمات المنشورة والمهمة عبر الإنترنت.
(4)	تطوير تقنيات الكشف المستخدمة وتصميمات الشبكة المطبقة والقدرة على فحص حركة المرور المشفرة .
(5)	أن تشمل أنظمة الكشف ما يلي: أ- أحداث التحذير،الرفض ، الحظر، ومنع التطفل المضمنة والمختلطة، سواءً على المضيف أو الشبكة. ب- أحداث التحذير ،الرفض ،الحظر على تقنيات تحليل الفيروسات والبرامج الضارة على المضيف أو الشبكة. ج- أحداث التحذير ،الرفض ،الحظر التي تتخذها أدوات كشف ومنع تسرب البيانات. د- وجود أدوات اختراق. هـ- الاستخدام والاستهلاك غير المعتاد لموارد النظام، بالإضافة إلى أعطال النظام. يُنصح بشدة باستخدام مستويات تفصيلية في مراقبة وجمع الإحصائيات لكل جلسة مستخدم ولكل عملية. و- الوصول إلى سجلات النظام والتطبيق، والتهيئة، والإعدادات، ومستودعات البيانات (مثل سجل (Windows)، وتعديلها. ز- السجلات والتنبيهات الصادرة عن أدوات التحقق من السلامة. ح- أنشطة الوصول على مستوى الخدمة، مثل:

	i. سلاسل من الطلبات والاستجابات لمورد خدمة ويب. ii. استعلامات (DNS) الصادرة والواردة. iii. طلبات وعقود(DHCP). iv. رسائل التصيد الاحتيالي المُبلغ عنها واستخدام خدمة البريد الإلكتروني.
8.3.5.2	**أمان البريد الإلكتروني (Email Security)**
المبدأ	تطوير وتحديث وتنفيذ وتوصيل سياسة وإجراءات استخدام البريد الإلكتروني.
الهدف	التحكم في الوصول إلى خدمات البريد الإلكتروني واستخدامها بناءً على حقوق وصول محددة ومُبرمجة بوضوح ومُمنوحة بناءً على احتياجات العمل.
الضوابط	
يجب علي الجهة وضع وتنفيذ الاجراءات الخاصة بالبريد الالكتروني وفق الآتي:	
(1)	الاستخدام المقبول لخدمات البريد الإلكتروني.
(2)	إرشادات للكشف عن رسائل التصيد الاحتيالي والبريد العشوائي، والتعامل الآمن مع المرفقات والروابط، والإرسال الآمن وإعادة التوجيه والرد.
(3)	الإلتزام بمتطلبات أمن البيانات وخصوصيتها. كما يجب إبلاغ المقاولين ومقدمي الخدمات الخارجيين والجهات الخارجية بها.
(4)	تزويد المستخدمين بأدوات وآليات ضرورية (مثل S/MIME) للتوقيع والتحقق رقمياً وتشفيروفك تشفير رسائل البريد الإلكتروني الفردية التي تحتوي على بيانات ومعلومات سرية للغاية ومؤثرة على العمل.
(5)	منع خدمة البريد من أن تكون "مُرسِلاً مفتوحاً" من خلال تحديد نطاقات أو عناوين الشبكة (IP) وموثوقة لإعادة توجيه رسائل البريد الإلكتروني.
(6)	فحص محتوى رسائل البريد الإلكتروني المتداولة والمتداخلة للكشف عن المرفقات الضارة والروابط المُضمَّنة.
(7)	الحماية من رسائل البريد الإلكتروني العشوائية ورسائل البريد الإلكتروني التي تحتوي على مُرسِلين ونطاقات وعناوين شبكة (IP) مُدرَجين في القائمة السوداء.
(8)	التحقق من صحة جلسات (SMTP) مع الأطراف الموثوقة باستخدام التشفير (TLS) إلى أقصى حد ممكن.

(9)	تطبيق سياسة الاحتفاظ بالبريد الإلكتروني وفقاً لسياسات الاحتفاظ بالبيانات وخصوصيتها.
8.3.6	**بيانات الأحداث والأدلة (Event Data and Evidences)**
8.3.6.1	**مزامنة الساعة (Time Synchronization)**
المبدأ	تطبيق آلية مزامنة الوقت لجميع أنظمة المعلومات والأمن السيبراني.
الهدف	ضمان تهيأة جميع الأنظمة لمزامنة تبادل المعلومات بينها.
الضوابط	
يجب علي الجهة ضبط مزامنة الانظمة وفق الآتي:	
(1)	وجود خدمة /خدمات وقت مركزية للجهة، حيث تُهيأ جميع الأنظمة لمزامنة معلومات الوقت معها.
(2)	مزامنة وقت خدمة /خدمات الوقت المركزية مع مصدرين وطنيين اودوليين موثوقين على الأقل.
(3)	تعتمد مصادر الوقت المُحددة على التوقيت العالمي المنسق (UTC).
(4)	حماية سرية معلومات الوقت المتبادلة وصحتها.
(5)	مراجعة سجلات ضبط الوقت على مكونات الشبكة والمخدمات ومراقبتها.
8.3.6.2	**جمع وتتبع مصادر الأحداث (Collecting and Tracking Event Sources)**
المبدأ	تجميع معلومات السجلات من كل المصادر بغرض التحليل.
الهدف	ضمان تجميع وتحليل معلومات السجلات والأحداث المجمعة من مصادر مختلفة إلى صيغة موحدة لتسهيل بناء قواعد التحليل والارتباط.
الضوابط	
يجب علي الجهة تجميع وتحليل السجلات وفق الآتي:	
(1)	تحديد نقاط مصدر الأحداث والسجلات محلياً وسحابياً. وأن تتضمن نقاط المصدر على الأقل ما يلي: أ- أجهزة ضوابط الأمن السيبراني التقنية، علي سبيل المثال لا الحصر (جدران الحماية، وأنظمة كشف ومنع التسلل، مراقبة التطبيقات، مكافحة الفيروسات، أدوات تحليل البرامج الضارة، أنظمة كشف ومنع تسرب البيانات، مراقبة قبول الشبكة، نقاط الوصول عن بُعد، وأدوات التحقق من السلامة).

	ب- أنظمة تشغيل المخدم والعميل. ج- التطبيقات، وأنظمة إدارة قواعد البيانات ، ومستودعات الملفات. د- الخدمات الأساسية للتطبيق (مثل مخدم الويب). هـ- إدارة الهوية وخدمات المصادقة. و- أجهزة الشبكة مثل المحولات، وأجهزة التوجيه، ونقاط الوصول. ز- خدمات الشبكة (مثل DHCP، وDNS، وخدمة البريد الإلكتروني). ح- أنظمة التحكم المادي (Physical Control Systems).
(2)	تحديد ما يجب جمعه من كل مصدر، على أن تتضمن معلومات الأحداث والسجلات المجمعة ما يلي: أ- إسم المستخدم (User ID). ب- تُوثيق جميع السجلات والأحداث المُجمعة بتواريخ وأوقات مُزامنة مع خدمة التوقيت المركزية. ج- مصدر ووجهة النشاط (الموقع، عنوان الشبكة (IP)، اسم المُضيف، مُعرّف العملية، اسم الخدمة، وغيرها). د- تفاصيل الحدث والإجراء، سواءً كان ناجحاً أم فاشلاً.
(3)	الإحتفاظ بالتسجيل (Log Retention) على النحو التالي: أ- أن تكون الأحداث والسجلات متاحةً وقابلةً للبحث لمدة عام على الأقل. ب- أن تكون حزم البيانات المُلتقطة من الشبكة متاحةً لإعادة بناء الجلسات لمدة أسبوعين على الأقل.
(4)	فحص الثغرات الأمنية، والتحديثات والتصحيحات المفقودة للأنظمة والتطبيقات.
(5)	إجراء عملية مراجعة دورية (مرتين سنوياً على الأقل)، لإعدادات التسجيل وتوثيقها.
(6)	تُجمع السجلات والأحداث في مستودع موحد وآمن، منفصل عن مصادر السجلات. كما يجب تطبيق تدابير لسلامة مستودع السجلات، ومنع مسؤولي تقنية المعلومات من التلاعب بها.
(7)	تحليل معلومات السجلات والأحداث المجمعة من مصادر مختلفة إلى صيغة موحدة لتسهيل بناء قواعد التحليل والارتباط.
(8)	عدم حذف السجلات الخام المجمعة، والاحتفاظ بها.
(9)	الاحتفاظ بدليل إرشادي لتحديد حالات الاستخدام التي يتم ترجمتها إلى قواعد تحليل وارتباط مستمرة وعند الطلب، لتمكين الكشف المبكر عن الأنشطة الضارة.

8.3.7	إدارة التهديدات السيبرانية (Cyber Threat Management)
المبدأ	تحديد وتقييم وفهم التهديدات التي تواجه أصول المعلومات، عبراستخدام مصادر وأنظمة موثوقة ومتعددة.
الهدف	ضمان الحصول على فهم مناسب لموقف التهديد الناشئ الذي تواجهه الجهة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد عملية إدارة معلومات التهديدات والموافقة عليها وتنفيذها.
(2)	قياس فعالية عملية إدارة معلومات التهديدات وتقييمها دورياً.
(3)	أن تشمل عملية إدارة معلومات التهديدات ما يلي: أ- استخدام المصادر الداخلية، علي سبيل المثال لا الحصر (التحكم في الوصول، سجلات التطبيقات البنية التحتية، نظام كشف التسلل (IDS)، نظام منع التطفل (IPS)، أدوات الأمن، مراقبة معلومات الأمن والأحداث (SIEM)، وظائف الدعم (الشؤون القانونية، التدقيق، التحليل الجنائي، إدارة الاحتيال، وإدارة المخاطر والإلتزام). ب- استخدام المصادر الخارجية الموثوقة مثل الهيئات الحكومية، منتديات الأمن، المنظمات الأمنية، وخدمات الإخطار المتخصصة. ج- اتباع منهجية محددة لتحليل معلومات التهديدات دورياً. د- جمع التفاصيل ذات الصلة بالتهديدات المحددة أو المجمعة، مثل أسلوب العمل، الجهات الفاعلة، الدوافع، ونوع التهديدات. هـ- أهمية المعلومات المُستقاة، وإمكانية اتخاذ إجراءات للمتابعة (مثل: مركز العمليات الأمنية (SOC)، وإدارة المخاطر). و- مشاركة المعلومات ذات الصلة مع أصحاب المصلحة المعنيين.
8.3.8	**الصيانة (Maintenance)**
المبدأ	وضع خطة شاملة للصيانة وفحوصات السلامة للمكونات بشكل دوري.
الهدف	ضمان إجراء عملية الصيانة علي جميع مستويات الأنظمة لتحسين الأداء والخدمات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	أن تكون جميع أصول تقنية المعلومات خاضعة لاتفاقيات صيانة أو تقديم خدمات سارية المفعول.
(2)	أن تتضمن الاتفاقيات شروط وأحكام الإستجابة والاسترداد، بما يتوافق مع مستويات حوجة العمل.
(3)	إجراء الصيانة الوقائية وفحوصات السلامة بشكل دوري لضمان الأداء وفقاً للغرض والمواصفات المحددة.
8.3.8.1	**منع تسريب البيانات (Data Leakage Prevention)**
المبدأ	التحكم في نقاط التسرب المحتملة من خلال تطبيق ضوابط الكشف عن تسرب البيانات والمعلومات، والتنبيه به، ومنعه.
الهدف	ضمان أمن البيانات أثناء النقل والمعالجة والتخزين، بحيث يجب على الجهة التحكم في نقاط التسرب المحتملة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد جميع النقاط التي قد تُسرب من خلالها البيانات والمعلومات السرية، سواءً عن قصد أو عن غير قصد. وقد تشمل نقاط التسريب المحتملة ما يلي: أ- مستوى نقاط النهاية والمضيفين، مثل ذاكرة فلاش (USB)، وأقراص (CD/DVD)، وغيرها. ب- مستوى خدمات الشبكة الداخلية والخارجية والتطبيقات المتصلة بالإنترنت، مثل النسخ والطباعة والبريد الإلكتروني وبروتوكولات (HTTP/S وSQL وSMB وFTP وSCP)، وغيرها ، ومتوفرة في كل من الموقع والسحابة. ج- المواد المادية، مثل الأوراق وغيرها.
(2)	ضمان أمن البيانات أثناء النقل والمعالجة والتخزين، يتعين على الجهة التحكم في نقاط التسرب المحتملة من خلال تطبيق ضوابط الكشف عن تسرب البيانات والمعلومات عبر عملية النقل وهي: أ- البيانات والمعلومات من خلال نقاط التسريب المحتملة بناءً على قواعد تصنيف مُحددة مسبقاً. ب- عبر نص عادي أو تنسيقات مُشفرة مع إعدادات افتراضية آمنة من الفشل.

(3)	في حالة حدوث خرق يؤثر على بيانات او معلومات الأعمال المصنفة، علي سبيل المثال لا الحصر (البيانات الشخصية، سجلات الموظفين، والبيانات المالية)، يجب على الجهة على الأقل: أ- تحديد نطاق الاختراق بوضوح ويشمل (أصحاب البيانات المتأثرين، وسمات البيانات المخترقة). ب- إجراء تقييم الأثر لتحديد ضوابط الاحتواء وتقدير تكلفة العواقب. ج- التواصل فوراً مع أصحاب البيانات المتأثرين في حال احتمالية أن يُسبب الاختراق مخاطر عالية، وذلك لتمكينهم من اتخاذ الاحتياطات اللازمة.
(4)	في حالة حدوث خرق يؤثر على البيانات والمعلومات الفنية السرية علي سبيل المثال لا الحصر(الكود المصدر، بيانات الاعتماد، تصميمات الشبكة الداخلية وتدفقات البيانات)، يجب على الجهة على الأقل: أ- تحديد الأنظمة والتطبيقات المتأثرة بوضوح. ب- التأكد من تصحيح جميع الثغرات الأمنية المعروفة وإجراء عمليات مسح جديدة لها. ج- التأكد من عدم وجود بيانات اعتماد مُرمزة. في حال وجود أي عيب فني، وتغيير جميع بيانات الاعتماد وكلمات المرور ومفاتيح المصادقة المُرمزة فوراً. د- تشفير بيانات الاعتماد وكلمات المرور ومفاتيح المصادقة المُرمزة بصيغ مُرمزة بشكل لا رجعة فيه أينما خُزنت ونُقلت. هـ- إجراء تقييم الأثر لتحديد ضوابط الاحتواء وتكلفة العواقب.
(5)	التواصل مع المقاولين ومقدمي الخدمات الخارجيين والأطراف الثالثة التي تعمل كأمناء ومعالجين للبيانات والمعلومات السرية لضمان التزامهم بالإجراءات المطبقة.
8.3.9	**استخدام الأجهزة الشخصية (Bring Your Own Device)**
المبدأ	ضمان حماية البيانات والمعلومات السرية أثناء نقلها وتخزينها عند استخدام الأجهزة الشخصية.
الهدف	منع تسرب أو سرقة البيانات الحساسة الخاصة بالجهة، علي سبيل المثال (البيانات المالية، خطط العمل، معلومات العملاء) المخزنة على أو المتاحة عبر الأجهزة الشخصية.
الضوابط	

يجب علي الجهة وضع ضوابط الأمن السيبراني لاستخدام الأجهزة الشخصية وفق الآتي:	
(1)	تمكين الوصول إلى موارد الشبكة الخاصة بالجهة من أجهزة غير مملوكة للجهة أو غير قابلة للتهيئة (Not configurable) وفقاً لمبادئ الثقة الصفرية.
(2)	تحديد مسؤوليات المستخدم، وعقد جلسات توعية حول مخاطر أمن الأجهزة الشخصية وضوابط الأمن السيبراني المطبقة عليها، والقيود والعواقب المترتبة على الموظفين.
(3)	تسجيل وإدارة الأجهزة الشخصية باستخدام حلول إدارة الأجهزة المحمولة (Mobile Device Management) التي تُمكن من الآتي: أ- تطبيق ضوابط أمنية بسلاسة. ب- تطبيق تقنيات العزل لفصل معلومات وتطبيقات الجهة عن المعلومات الشخصية. ج- تطبيق ضوابط الوصول وآلية التشفير، بالإضافة إلى منع تسريب البيانات غير المصرح بها. د- مسح البيانات والمعلومات والتطبيقات المشغلة عن بُعد.
(4)	تحديد عدد الأجهزة الشخصية التي يستخدمها كل موظف بناءً على احتياجات العمل.
(5)	الموافقة المسبقة على تطبيقات الهاتف المحمول العامة والخاصة بالجهات الخارجية التي يمكنها الوصول إلى أصول معلومات الجهة.
(6)	حظر الوصول من الأجهزة المفقودة أو التي تم اختراقها أو التي تعرضت لاختراق الحماية، بالإضافة إلى الموظفين المفصولين.
(7)	تسجيل أنشطة وصول الأجهزة الشخصية ومراقبتها.
8.3.10	**إدارة الثغرات واختبار الاختراق (Vulnerabilities Management and Penetration Testing)**
8.3.10.1	**إدارة الثغرات (Vulnerabilities management)**
المبدأ	تطويروتنفيذ وتوصيل سياسة وإجراءات إدارة الثغرات في البنية الأساسية والتطبيقات والتعاملات.
الهدف	العثور على الثغرات وتحديدها في الأنظمة والبرامج والشبكات بشكل استباقي ومستمر والتعرف عليها في الوقت المناسب ومعالجتها بشكل فعال.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	أن تتضمن سياسة وإجراءات إدارة الثغرات الأمنية، الأصول وجميع عناصر التهيئة المحددة مثل الآتي: أ- مشرف الأجهزة الافتراضية، وأنظمة التشغيل، والبرامج الثابتة، وبرامج التشغيل. ب- تطبيقات المخدمات، وسطح المكتب، والهواتف المحمولة، بالإضافة إلى البرامج الوسيطة وأنظمة إدارة قواعد البيانات . ج- أجهزة ومكونات الشبكة.
(2)	أن تتضمن منهجيات تحديد نقاط الضعف ما يلي على الأقل: أ- عملية دورية لربط وإيجاد تطابقات بين معدات(CPE) المُخزنة، ومعدات (CVE) المنشورة، وأنظمة (CVSS) ذات الصلة. ب- تلقي الإشعارات من الموردين والشركاء الخارجيين وفرق الإستجابة لطوارئ الحاسب الآلي (CERTs) عبر قنوات موثوقة مثل رسائل البريد الإلكتروني، وبوابات الموردين أو مقدمي الخدمات، وبرامج إدارة التصحيحات. ج- نتائج عمليات فحص الثغرات الأمنية واختبار الاختراق، بالإضافة إلى ضوابط الأمن السيبراني الأخرى.
(3)	تحديد ضوابط تصحيحية ممكنة بناءً على توصيات (CVE) والموردين. قد تؤثر هذه الضوابط التصحيحية سلباً على تطبيقات الأعمال وعملياتها. في هذه الحالة يجب تحديد ضوابط تعويضية، وإذا لم تكن قابلة للتطبيق، يجب إجراء عملية تقييم للمخاطر.
(4)	أن تتم المعالجة من خلال عملية إدارة التغيير المعتمدة.
(5)	أن يُراعى عند تصنيف الثغرات الأمنية وتحديد أولوياتها ما يلي: أ- قيمة درجة (CVSS)، ومستوى التعرض لحدث تهديد، وما إذا كانت الثغرة قد استُغلت سابقاً. ب- نوع وموقع الأصل المعرض للخطر (مثل: الإنترنت أو التعامل مع الجمهور، أو التواصل مع شبكات أو جهات غير موثوقة، أو نظام إدارة قواعد البيانات ، أو نظام الأمان، وغيرها). ج- وزن الأصل المعرض للخطر بناءً على خطورته ودرجة حساسيته.
(6)	إنشاء عمليات مسح الثغرات الأمنية واختبار الاختراق والحفاظ عليها. مع مراعاة ما يلي: أ- تحديد وتيرة إجراء عمليات فحص الثغرات الأمنية.

	ب- تحديد وتيرة إجراء الفحص وفقًا لخطورة وحساسية الأنظمة، بالإضافة إلى أفضل الممارسات واللوائح ذات الصلة وقواعد القطاع. ج- إجراء الفحص مرة واحدة شهريًا على الأقل للأنظمة الحرجة والحساسة.
(7)	تحديد نطاق كل عملية مسح، وأن تشمل على الأقل: أ- مكونات الأنظمة والبنية التحتية ضمن نطاق الفحص. ب- نطاق وعمق تغطية الفحص لكل نظام. يُشير النطاق إلى نسبة المكونات أو عدد الثغرات الأمنية المطلوب فحصها، بينما يُشير العمق إلى مستوى تصميم النظام المطلوب فحصه.
(8)	استخدام آليات لتحليل عمليات مسح الثغرات الأمنية المتعددة بمرور الوقت لتحديد اتجاهات ثغرات النظام وأنماط الهجمات.
(9)	مراجعة سجلات التدقيق التاريخية لتحديد ما إذا كان المهاجمون قد استغلوا سابقاً الثغرات الأمنية المكتشفة حديثاً في الأنظمة.
(10)	ربط مخرجات عمليات مسح الثغرات الأمنية للتحقق من وجود مصادر هجوم متعددة تم تحديدها من خلال عملية نمذجة التهديدات.
8.3.10.2	**اختبار الإختراق (Penetration Test)**
المبدأ	إجراء اختبارات الاختراق وفقاً لأهمية وحساسية الأنظمة، بالإضافة إلى أفضل الممارسات واللوائح ذات الصلة.
الهدف	إجراء اختبار لتجاوز ضوابط الامن السيبراني المطبقة ،لتحديد درجة مقاومتها للاختراق والهجمات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد وتيرة إجراء عمليات اختبار الاختراق.
(2)	تحديد نطاق كل عملية اختبار.
(3)	استخدام نتائج عملية فحص الثغرات الأمنية لدعم اختبار الاختراق.
(4)	أن تُدار عملية اختبار الإختراق من قبل فريق مستقل.
(5)	إبلاغ قواعد الإشتباك والعقود، وحماية البيانات والمعلومات السرية.
(6)	إجراء الاختبار بتجاوز الضوابط المطبقة ومن خلالها لتحديد درجة مقاومتها للاختراق والهجمات ،على أن يشمل محاولات تجاوز ضوابط الأمن المادية المطبقة.

(7)	أن تأخذ عملية الاختبار في الاعتبار تنفيذ هجمات قائمة على التكنولوجيا (مثل التفاعلات مع الأنظمة والعمليات)، وهجمات قائمة على الهندسة الاجتماعية (مثل التفاعلات عبر البريد الإلكتروني والهاتف). مع مراعاة التكتيكات والتقنيات والإجراءات والأدوات العدائية.
(8)	مراعاة حماية البيانات واستمرارية الخدمة أثناء إجراء عمليات فحص الثغرات الأمنية واختبار الاختراق العدواني لضمان عدم انقطاع الخدمة وعدم فقدان البيانات.

9. الأمن السيبراني للخدمات المالية الرقمية (Digital Services and Transaction)

9.1	**الخدمات والمعاملات الرقمية (Digital Services and Transaction)**
9.1.1	**حماية بيانات العملاء والمعاملات (Protection of Customer Data and Transactions)**
المبدأ	حماية بيانات العملاء والمعاملات من الوصول أو الإستخدام أو التعديل أو الإفصاح غير المصرّح به، من خلال تطبيق ضوابط أمنية وتقنية فعالة.
الهدف	تعزيز سرية وسلامة وخصوصية بيانات العملاء في جميع مراحل المعالجة والتخزين والنقل، بما يدعم الثقة في الخدمات المصرفية الرقمية ويضمن الإلتزام للمتطلبات التنظيمية والمعايير الدولية لحماية البيانات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تطبيق آليات تشفير قوية وآمنة لحماية البيانات الحساسة أثناء التخزين والنقل، بما يضمن سريتها وسلامتها.
(2)	منع تخزين بيانات حساسة مثل كلمات المرور أو أرقام البطاقات بصيغ غير مشفّرة أو قابلة للقراءة.
(3)	تفعيل المصادقة متعددة العوامل (MFA) في عمليات تسجيل المستخدمين، إدارة المستفيدين، المعاملات ذات المبالغ الكبيرة، وتغيير بيانات الإتصال.
(4)	الإشعار الفوري للعميل بأي معاملة مالية أو تغيير في الإعدادات أو معلومات الحساب، باستخدام قنوات موثوقة (SMS) / بريد إلكتروني.

(5)	منع استخدام كلمات مرور ضعيفة، وفرض سياسات كلمات مرورة قوية و معقدة وفترات صلاحية لتغييرها.
(6)	اعتماد تقنيات عدم التخزين المؤقت (Non-caching) للبيانات السرية في التطبيقات البنكية، خاصة على الأجهزة المحمولة.
(7)	استخدام آليات التحقق من الجهاز (Device Binding) وربط المعاملات بأجهزة محددة موثوقة.
(8)	تقييد الوصول إلى بيانات العملاء وفق مبدأ "أقل صلاحية (Least Privilege Access)".
(9)	تنفيذ سجل تدقيق (Audit Log) للعمليات على بيانات العملاء مع حماية هذه السجلات من التعديل أو الحذف.
(10)	مراجعة دورية لسياسات الخصوصية و الإلتزام بلوائح حماية البيانات مثل (GDPR) والقوانين المحلية وموجهات بنك السودان المركزي.
9.1.2	**التوعية الأمنية (Security Awareness)**
المبدأ	تعزيز الوعي الأمني لدى العاملين والعملاء لتمكينهم من التعرف على المخاطر السيبرانية وتبنّي ممارسات رقمية آمنة تسهم في الحد من محاولات الإحتيال والهجمات السيبرانية.
الهدف	ترسيخ الثقافة الأمنية باعتبار العنصر البشري خط الدفاع الأول في حماية الأنظمة والمعلومات من التهديدات السيبرانية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تنفيذ حملات توعوية دورية عبر قنوات التواصل الرسمية للجهة، تتضمن كيفية: أ- تجنب مشاركة كلمات المرور أو الرموز السرية. ب- تثبيت التطبيقات فقط من خلال المواقع الرسمة للجهة و متاجر التطبيقات المعتمدة. ج- الإبلاغ الفوري عن أي تغيير في بيانات التواصل. د- تجنب الضغط على الروابط أو فتح المرفقات المشبوهة.

9.2	أمن التطبيقات والقنوات الرقمية (Application and Digital Channel Security)
المبدأ	دمج متطلبات الأمن السيبراني في مراحل تصميم وتطوير وتشغيل التطبيقات والقنوات الرقمية، لضمان سرية وموثوقية الخدمات الرقمية وتقليل احتمالات الإستغلال أو الإختراق.
الهدف	تأمين التطبيقات والقنوات الرقمية ضد الثغرات والهجمات السيبرانية عبر تطبيق مبدأ "الأمن المدمج منذ التصميم".
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تطوير كافة القنوات البنكية الرقمية (الموبايل، الإنترنت، الهاتف المصرفي) وفقاً لمبدأ الأمن المدمج منذ التصميم (Security by Design).
(2)	منع تثبيت التطبيقات البنكية على أجهزة غير آمنة (Rooted/Jailbroken) أو معدّلة، والتحقق من سلامة الجهاز عند كل تسجيل دخول.
(3)	التأكد من أن تحميل وتثبيت التطبيقات يتم حصراً عبر القنوات الرسمية والمعتمدة، مع نشر روابط التحميل على منصاتها الرسمية فقط.
(4)	إنهاء الجلسات تلقائياً بعد فترة محددة من عدم النشاط، وتقييد عدد الجلسات النشطة لكل حساب.
(5)	تبني أحدث تقنيات الحماية لتأمين قنوات الإتصال الإلكترونية ضد الهجمات، على سبيل المثال هجمات الرجل في المنتصف (MiTM).
(6)	تجنب تخزين أي بيانات حساسة في ذاكرة التطبيق أو الجهاز مثل كلمات المرور أو الرموز.
(7)	التحقق من رقم الهاتف وجهاز العميل (IMEI/Device Binding) عند تسجيل الدخول لأول مرة.
(8)	تطبيق حماية ضد التصيد الإلكتروني (Phishing) من خلال رسائل توعية، وتحذيرات داخل التطبيق، وربطها بأنظمة كشف الروابط المزيفة.
(9)	التأكد من توثيق سياسات الإستخدام في إتفاقيات واضحة بين الجهة والعميل، توضح المسؤوليات والإلتزامات الأمنية من الطرفين.
(10)	إعلام العملاء مسبقاً بأي توقف مجدول أو تحديث تقني، وتوفير قناة بديلة آمنة للعمليات المهمة.

(11)	إجراء تقييم أمني دوري للتطبيقات والمنصات الإلكترونية، يشمل إختبارات إختراق وإختبارات توافق الأجهزة.
9.3	**حماية القنوات البديلة ووسائل الإتصال (Protection of Alternative Channels and Communication Means)**
المبدأ	تأمين القنوات البديلة ووسائل الإتصال ضد الإحتيال والإنتحال عبر مصادقة متعددة العوامل وتشفير الإتصالات والتحقق المستمر من هوية العملاء.
الهدف	تعزيز أمان القنوات البديلة ووسائل الإتصال لضمان استمرارية الأعمال والحفاظ على سرية وسلامة بيانات العملاء والتقليل من مخاطر الإحتيال السيبراني أثناء التفاعل عبر القنوات المختلفة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	توثيق العمليات الحساسة باستخدام مصادقة ثنائية مستقلة علي سبيل المثال لا الحصر (OTP) عبر قناة منفصلة.
(2)	تطبيق تحقق صارم لهوية العميل في الإتصالات الهاتفية، مع تجنب استخدام أسئلة تحقق تقليدية أو متوقعة.
(3)	الحد من استخدام قنوات غير مشفرة لنقل بيانات حساسة (مثل البريد أو منصات التواصل الإجتماعي).
(4)	إعتماد تقنيات كشف ومنع التصيّد والإنتحال، وربطها بتحذيرات داخل التطبيقات والمنصات.
(5)	فرض تحقق إضافي عند تغيير معلومات الإتصال، مع إشعار المستخدم عبر وسيلة الإتصال المعتمدة لدى الجهة.
(6)	تسجيل كافة الإتصالات عبر القنوات البديلة لأغراض التدقيق والإلتزام.
(7)	تضمين رسائل تنبيهية دائمة داخل التطبيقات لتحذير العملاء من مشاركة المعلومات الحساسة.
9.4	**عمليات البطاقات (Card Operations)**
المبدأ	إصدار وتفعيل وتشغيل البطاقات وفق معايير أمان معتمدة، مع تطبيق ضوابط للتحقق من هوية العملاء وتأمين أجهزة الدفع ضد العبث والإحتيال.

الهدف	تعزيز حماية بيانات ومعاملات البطاقات وضمان سلامة وأمن بيئة الدفع الإلكتروني عبر مراقبة مستمرة وكشف مبكر للأنشطة المشبوهة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إصدار البطاقات في حالة غير مفعّلة، وتفعيلها فقط بعد التحقق من هوية العميل عبر قنوات معتمدة.
(2)	تأمين أجهزة الصراف الآلي ونقاط البيع ضد محاولات التلاعب من خلال: أ- تقنيات ضد الإحتيال المالي (Skimming). ب- حماية لوحة إدخال الرقم السري (PIN Pad Protection). ج- المراقبة المرئية :تلتزم الجهة بتركيب وتشغيل أنظمة (CCTV) لمراقبة وحماية المنشآت والأصول. د- كشف التوصيلات غير المصرح بها علي سبيل المثال لا الحصر (USB Ports) أو أسلاك التعديل.
(3)	تطبيق آليات لإيقاف أجهزة الدفع عن بُعد عند اكتشاف نشاط مشبوه.
(4)	حظر البطاقة تلقائياً بعد عدد محدد من محاولات التوثيق الفاشلة.
(5)	الإلتزام بمعايير الأمان المعتمدة علي سبيل المثال لا الحصر PCI ، DSS لحماية بيانات البطاقات والمعاملات.
9.5	**كشف الإحتيال (Fraud Detection)**
المبدأ	تطبيق أنظمة مراقبة وتحليل فعّالة لرصد الأنشطة غير الطبيعية واكتشاف محاولات الإحتيال في الوقت المناسب، مع الإستفادة من التقنيات الحديثة وتحديث معلومات التهديدات بشكل دوري.
الهدف	تعزيز حماية العملاء والمعاملات من الإحتيال والإختراقات عبر الكشف المبكر والإستجابة السريعة والتواصل الفوري عند رصد الأنشطة المشبوهة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	استخدام أنظمة مراقبة ذكية وفورية (Real-time Fraud Detection) تعتمد على التحليلات السلوكية لرصد الأنشطة المشبوهة.

(2)	تفعيل آليات مراقبة الأجهزة الطرفية مثل أجهزة الصراف الآلي (ATM) ونقاط البيع (POS) لرصد أي سلوك غير معتاد، مثل إدخال أجهزة خارجية أو إعادة التشغيل غير المصرّح به، وتطبيق ضوابط الأمن السيبراني على البنية التحتية، بما يشمل حماية أنظمة التشغيل، وكشف البرمجيات الخبيثة، واستخدام تقنيات ضد الاحتيال المالي (Anti-skimming) وربط هذه الآليات بمنصة مركزية للجهة لتحليل الأحداث وتنبيه الفرق المختصة عند اكتشاف تهديدات محتملة.
(3)	تنفيذ تحليل ما بعد الحادث (Post-Incident Analysis) لأي حالة إحتيال أو إختراق لتحديد الثغرات وتحديث الإجراءات الوقائية.
(4)	دمج تقنيات الذكاء الإصطناعي وتعلم الآلة في أنظمة المراقبة لتقليل الإنذارات الكاذبة وتحسين دقة الكشف.
(5)	تحديث مستمر لقواعد بيانات التهديدات السيبرانية (Threat Intelligence) وربطها بمنظومة المراقبة.
(6)	إعداد سيناريوهات تنبيه آلي (Alerts) عند تجاوز حدود أو أنماط محددة من المخاطر، مثل تكرار محاولات الدخول أو المعاملات غير الإعتيادية.
(7)	تلتزم الجهة بربط أنظمة كشف الإحتيال بمنصات الإشعارات الفورية لإخطار العملاء بشكل مباشر عند رصد أي معاملات غير مألوفة.
(8)	تمكين العملاء من حظر بطاقاتهم أو حساباتهم مباشرةً من خلال القنوات الرقمية أو مركز الخدمة.
(9)	تدريب دوري لموظفي خدمة العملاء على اكتشاف العلامات المبكرة لمحاولات الإحتيال أو الإختراق.
(10)	استخدام أنظمة مراقبة ذكية وفورية (Real-time Fraud Detection) تعتمد على التحليلات السلوكية لرصد الأنشطة المشبوهة.
9.6	**الإلحاق الرقمي (Digital Onboarding)**
المبدأ	تطبيق ضوابط تحقق متعددة المستويات للتأكد من هوية العميل.
الهدف	تحقيق إلحاق رقمي (فتح الحسابات المصرفية عن بعد) آمن وموثوق يمنع التزوير ويعزز الثقة في الخدمات المصرفية الرقمية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	التأكد من الهوية من خلال: أ- التحقق من صحة المستندات المقدمة عبر خصائص الأمان المادية أو الجهات المصدرة الرسمية. ب- مطابقة الصورة الحية (Selfie) مع صورة الهوية باستخدام تقنيات التحقق البيومتري. ج- التحقق من صحة البيانات عبر مصادر موثوقة .
(2)	الكشف عن التزوير أو الإنتحال: أ- تطبيق آلية التحقق من الهوية و إجتياز إختبار الكشف عن الحيوية (Liveness Detection). ب- استخدام خوارزميات تحقق معتمدة دولياً مثل (ISO/IEC 30107-3). ج- التأكد من أن الشخص لم يقم بالتسجيل مسبقًا باستخدام تقنية مقارنة السمات الحيوية (Biometric Deduplication) .
(3)	تأمين قنوات الإلحاق: أ- التحقق من الموقع الجغرافي وقت الإلحاق لأغراض مكافحة الإحتيال (إضافه إرسال التنبيهات بمحاولات الدخول من موقع مختلف). ب- توثيق عملية الإلحاق بمقابلة الفيديو المرئية أو التوقيع الرقمي.
9.7	**إشعار العملاء (Customer Notification)**
المبدأ	إرسال إشعارات فورية وآمنة للعملاء عند تنفيذ المعاملات أو التغييرات الجوهرية في الحساب، دون تضمين بيانات حساسة.
الهدف	تمكين العملاء من الإستجابة السريعة لأي نشاط غير معتاد وتعزيز الشفافية وحماية الحسابات من الإحتيال.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إرسال إشعارات فورية وآمنة عبر قنوات معتمدة) مثل SMS أو البريد الإلكتروني (عند تنفيذ معاملات مالية أو تغييرات مهمة في الحساب (إضافة مستفيد، تغيير معلومات الإتصال، محاولات دخول فاشلة، أو معاملات مشبوهة/ذات المبالغ الكبيرة).
(2)	إرسال الإشعارات إلى الرقمين (القديم والجديد) عند تغيير رقم الهاتف، والبريد الإلكتروني كإجراء أمني.

(3)	منع تضمين بيانات حساسة في الإشعارات، مثل الرقم الكامل للبطاقة أو الحساب.
(4)	إتاحة قنوات آمنة وسريعة للعملاء لحظر البطاقات أو الإبلاغ عن الأنشطة المشبوهة.

10. إدارة الأزمات والتخطيط للطوارئ (Crisis Management and Emergency Planning)

10.1	إدارة الأزمات السيبرانية (Cyber Crises Management)
المبدأ	تطبيق نهج شامل ومتكامل لإدارة الأزمات السيبرانية يضمن الإستعداد المسبق، والإستجابة الفعّالة، والتعافي السريع، من خلال خطط معتمدة ومحدثة، وأدوار ومسؤوليات واضحة، وتنسيق داخلي وخارجي منسق، بما يعزز صمود الجهة ويحافظ على استمرارية أعمالها.
الهدف	ضمان تفسير موحد، واستعداد، وإستجابة، وتعافي متسق طوال دورة حياة الأزمة، مع اعتماد برنامج إدارة أزمات مناسب.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	الحفاظ على خطط إدارة أزمات محدثة تدعم صمود الجهة بما يتجاوز إدارة الأزمات السيبرانية. كما يجب أن تكون هذه الخطط: أ- معتمدة من مجلس الإدارة أو الإدارة العليا. ب- مطبقة على مستوى الجهة لضمان تغطية الوظائف التنظيمية الرئيسية، والصلاحيات، والمسؤوليات. ج- متوافقة مع المتطلبات القانونية والتنظيمية الداخلية والخارجية ومتوافقة مع اعتبارات إدارة المخاطر التشغيلية (مثل: التعافي من الكوارث، استمرارية الأعمال، وسياسات وخطط وإجراءات وقنوات الإتصالات الداخلية والخارجية).
(2)	تحديد فريق إدارة الأزمات الذي يدمج وظائف التقنية وإدارة الأعمال.
(3)	تحديد مسؤول عن فريق ادارة الازمات من قبل الجهه، ويضم ممثلين مخولين من العمليات، وتقنية المعلومات / أمن المعلومات،والشؤون القانونية، والإتصالات. ويجب على الفريق أن:

	أ- يطور، يحدث، يروج، ويمارس خطط إدارة الأزمات. ب- يساعد مسؤول فريق إدارة الأزمات لتقييم ما إذا كان هناك حادث ذو تأثير أزمة ويتطلب إستجابة رسمية. ج- يهيئ وينشر الموارد الداخلية والخارجية اللازمة لتنفيذ الإستجابة. د- يشرف على تنفيذ أنشطة الإستجابة. هـ- يدير الإتصالات مع أصحاب المصلحة الداخليين والخارجيين طوال دورة حياة إدارة الأزمة.
(4)	التأكد من أن مسؤول الإستجابة للأزمات لديه: أ- المهارات والخبرة لفهم عمليات الجهة واتخاذ القرارات. ب- اجتياز التدريب المناسب (مثل الحصول على المؤهلات ذات الصلة) حول التوجهات الجديدة المتعلقة بالأزمات السيبرانية. ج- السلطة والمسؤولية لاتخاذ القرارات بشكل مستقل أثناء الإستجابة للأزمة.
(5)	توثيق عملية إدارة الأزمات السيبرانية، والموافقة عليها، واختبارها، وتحديثها بشكل دوري. وأن تتضمن العملية: أ- معالجة اعتبارات إدارة المخاطر التشغيلية (مثل التعافي من الكوارث، استمرارية الأعمال، وسياسات وخطط وإجراءات وقنوات الإتصالات الداخلية والخارجية). ب- تغطية الجهة بأكملها لضمان شمول الوظائف التنظيمية الرئيسية، والصلاحيات، والمسؤوليات.
(6)	تحديد مصفوفة شدة التأثير معتمدة من مجلس الإدارة أو الإدارة العليا. كما يجب أن: أ- يتم الأخذ في الإعتبار نتائج تحليلات تأثير الأعمال الخاصة بالجهة، والتقييمات الداخلية، وتحليلات المخاطر. ب- تصنف التأثير على الجهات المنظمة (مثل منخفض، متوسط، عالي، طفيف، معتدل، شديد،وغيرها) عبر فئات الإعتبار المهمة، بما يتماشى مع المخاطر السيبرانية الكلية. ج- تحدد الإجراءات التخفيفية المناسبة لكل مستوى تأثير.

(7)	تطبيق وصيانة الأدوات المناسبة وتغذيات مصادر التهديدات من الأنظمة الداخلية ومزودي الطرف الثالث لمساعدتها في بدء جهود الإستجابة للمخاطر على مستوى الجهة عند الحاجة.
(8)	تنفيذ آليات إعلام طارئة لدعم الإتصال السريع بالمستجيبين والموظفين في حال وقوع حادث ذو تأثير أزمة.
(9)	أن تستخدم أدوات لإدارة الأزمات (مثل تسجيل القرارات والإجراءات) لإنشاء سجل يمكن مراجعته ويساعد في تحسين الإستجابة بناءً على الدروس المستفادة.
(10)	أن تعتمد نموذج تعلم مستمر لتحسين جاهزيتها المستقبلية للحوادث السيبرانية.
(11)	أن توفر: أ- تدريب منتظم يناسب أدوار المستجيبين في إدارة الأزمات. ب- تدريب فوري عند حدوث أي تغيير في عملية الإستجابة.
(12)	أن تقوم الجهة باختبارات للأزمات السيبرانية سنوياً لضمان فعالية خطط وإجراءات إدارة الأزمات.
(13)	أن تشارك الجهة في اختبارات أزمات القطاع المصرفي التي ينظمها بنك السودان المركزي والتي ترتكز على سيناريوهات محددة.
(14)	أن تبلغ عن الحوادث حسب التالي: أ- الحوادث منخفضة الخطورة تُبلغ بصورة ربع سنوية. ب- الحوادث متوسطة الخطورة تُبلغ خلال 8 ساعات عمل من تأكيدها. ج- الحوادث عالية الخطورة تُبلغ خلال 4 ساعات من تأكيدها.
(15)	أن تحدث معلومات الحوادث حسب التالي: أ- الحوادث متوسطة الخطورة يتم تحديثها كل يومين عمل. ب- الحوادث عالية الخطورة يتم تحديثها يومياً.
(16)	أن تبلغ عن الحوادث باستخدام الإستمارات والقنوات المحددة مسبقاً.
(17)	أن تشارك وتتعاون في الإستجابة للأزمات السيبرانية في القطاع المصرفي حسب الخطورة والإجراءات التي يحددها بنك السودان المركزي.

10.2	إدارة الحوادث وخطط الإستجابة (Incident Management and Response Plans)
المبدأ	التعرف والإستجابة السريعة والفعالة والمنظمة لحوادث الأمن السيبراني، لتقليل الأثر المحتمل أو الفعلي على أعمال الجهه.
الهدف	تعريف واعتماد وتنفيذ عملية لإدارة حوادث الأمن السيبراني، تكون متماشية مع عملية إدارة الحوادث المؤسسية، وذلك من أجل التعرف على حوادث الأمن السيبراني والإستجابة لها والتعافي منها. ويجب قياس فعالية هذه العملية وتقييمها بشكل دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد، الموافقة على، وتنفيذ عملية إدارة حوادث الأمن السيبراني، وتقييم ومراجعة هذه العملية بشكل دوري.
(2)	أن تأخذ عملية إدارة حوادث الأمن السيبراني في الإعتبار المتطلبات التالية: أ- بناء فريق مخصص يكون مسؤولاً عن إدارة حوادث الأمن السيبراني مع تحديد أدوار ومسؤوليات الفريق المشاركين في عملية الإدارة. ب- إنشاء عملية لإدارة الحوادث تُمكّن الجهه من التعامل مع حوادث الأمن السيبراني. قد تشمل العملية التوثيق، والكشف، والفرز، والتصنيف، والتحليل، والتواصل، والتنسيق مع الأطراف المعنية. ج- إنشاء عملية لتحديد التدريبات والشهادات والتطوير المهني المستمر اللازم لفريق الإستجابة للحوادث. د- إنشاء مستودع لتوثيق حوادث الأمن السيبراني.
(3)	وضع عملية لأداء المهام الجنائية الرقمية (التحقيقات الجنائية الإلكترونية) ويجب توفر سعة كافية داخل الفريق المعتمد للقيام بالتعامل مع الحوادث الكبرى.
(4)	وضع عملية للتعامل مع الأدلة ذات الصلة وحمايتها.
(5)	أن تتضمن عملية إدارة الحوادث تحليل السبب الجذري وتحليل الأثر، بالإضافة إلى اتخاذ الإجراءات التصحيحية والوقائية اللازمة.
(6)	تسجيل جميع حوادث الأمن السيبراني ومراقبتها ومعالجتها بشكل مناسب ضمن الأطر الزمنية المحددة للحل.

(7)	احتواء تأثير أي هجمات سيبرانية من خلال تنفيذ ضوابط الحماية أو عزل الأجهزة/الأنظمة المتأثرة حسب الإقتضاء.
(8)	أن تساعد استجابات التخفيف الجهة على منع تفاقم الوضع وتجنب الحوادث السيبرانية لتقليل الأثر على عمليات وخدمات الجهه.
(9)	توثيق وتسجيل الإجراءات المتخذة من وقت اكتشاف الحادث وحتى حله النهائي مع تحديد الوقت بدقة.
(10)	أن يكون هناك آلية لمشاركة معلومات الحوادث السيبرانية، خاصة الحوادث الحرجة.
(11)	وضع وتنفيذ خطط لتعزيز الصمود وإستعادة الخدمات التي تضررت نتيجة للأحداث السيبرانية.
(12)	الحفاظ على إجراءات وعمليات التعافي وتنفيذها لضمان إستعادة الأصول والأنظمة المتأثرة بالحوادث السيبرانية بشكل صحيح.
(13)	وضع عملية لتحسين خطط الإستجابة والتعافي من خلال الإستفادة من الدروس المستفادة من أنشطة الكشف والإستجابة الحالية والسابقة، ويجب تحويل هذه الدروس إلى ضوابط وتعزيزات إجرائية.
(14)	بناء دراسات حالة عن الحوادث السيبرانية السابقة لإستخدامها خلال جلسات التدريب.
(15)	استعادة عمليات الأعمال مع ضمان أمن العمليات والبيانات/المعلومات.
(16)	دمج مخاطر الأمن السيبراني الناجمة عن مزودي الخدمات من الطرف الثالث بشكل مناسب ضمن تقييم المخاطر السيبرانية للجهات.
10.2.1	**إدارة التهديدات (Threat Management)**
المبدأ	الحصول على فهم كافٍ للوضع الحالي والمتطور للتهديدات التي تواجه الجهة.
الهدف	تحديد واعتماد وتنفيذ عملية لإدارة معلومات التهديدات، بهدف التعرف على التهديدات التي تواجه أصول المعلومات التابعة لها، وتقييمها وفهمها، وذلك باستخدام مصادر متعددة وموثوقة. ويجب قياس فعالية هذه العملية وتقييمها بشكل دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد واعتماد وتنفيذ عملية إدارة معلومات التهديدات.
(2)	قياس فعالية عملية إدارة معلومات التهديدات وتقييمها بشكل دوري.
(3)	أن تتضمن عملية إدارة معلومات التهديدات ما يلي:

	أ- استخدام المصادر الداخلية، مثل: سجلات التحكم في الوصول، سجلات التطبيقات والبنية التحتية، أنظمة كشف التسلل (IDS)، أنظمة منع التسلل (IPS)، أدوات الأمان، نظام إدارة معلومات وأحداث الأمان (SIEM)، والوظائف الداعمة (مثل: الشؤون القانونية، التدقيق، مكتب دعم تكنولوجيا المعلومات، التحقيقات الجنائية، إدارة الإحتيال، إدارة المخاطر، والإلتزام). ب- استخدام مصادر خارجية موثوقة وذات صلة، مثل: بنك السودان المركزي، الجهات الحكومية، المنتديات الأمنية، مزودي خدمات الأمان، المنظمات الأمنية، وخدمات الإخطار المتخصصة. ج- منهجية محددة لتحليل معلومات التهديدات بشكل دوري. د- التفاصيل ذات الصلة حول التهديدات المحددة أو المجمعة، مثل: أسلوب العمل، الجهات الفاعلة، الدوافع، وأنواع التهديدات.
10.2.2	**إدارة الثغرات الأمنية (Vulnerability Management)**
المبدأ	التعرف على الثغرات في التطبيقات والبنية التحتية ومعالجتها بشكل فعّال وفي الوقت المناسب، وذلك لتقليل إحتمالية وقوعها وتأثيرها على أعمال الجهة.
الهدف	تحديد واعتماد وتنفيذ عملية لإدارة الثغرات الأمنية، بهدف التعرف على الثغرات في التطبيقات والبنية التحتية ومعالجتها. مع قياس فعالية هذه العملية وتقييمها بشكل دوري.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد وإعتماد وتنفيذ عملية إدارة الثغرات الأمنية.
(2)	قياس فعالية عملية إدارة الثغرات الأمنية وتقييمها بشكل دوري.
(3)	أن تتضمن عملية إدارة الثغرات الأمنية ما يلي: أ- جميع أصول المعلومات. ب- وتيرة إجراء فحص الثغرات (بناءً على المخاطر). ج- تصنيف الثغرات الأمنية د- جداول زمنية محددة للمعالجة (لكل تصنيف). هـ- تحديد الأولويات لأصول المعلومات المصنفة.

	و- إدارة التحديثات (Patch Management) وطريقة نشرها.
10.3	**عملية إدارة الحوادث (Incident Management Process)**
المبدأ	الإستجابة الفورية والفعّالة للحوادث الأمنية السيبرانية وفق الأُطر الزمنية المحددة، ومتابعتها حتى معالجتها وإستعادة العمليات إلى وضعها الطبيعي بكفاءة عالية.
الهدف	ضمان الإستجابة الفعّالة والمنسقة للحوادث الأمنية السيبرانية، بحيث يتم الإبلاغ عنها في الوقت المناسب، والحد من تأثيرها، واستعادة الأنظمة والخدمات المتأثرة بشكل آمن وسريع.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تقديم تقرير رسمي بجميع الحوادث السيبرانية إلى بنك السودان المركزي وفقاً للجداول الملحقة في هذا الإطار، وذلك على النحو التالي: أ- إخطار بنك السودان المركزي فوراً عند وقوع حادث سيبراني مرتفع الشدة، وذلك خلال 4 ساعات كحد أقصى من تأكيد الحادث. (ملحق رقم 4) ب- إخطار بنك السودان المركزي فوراً عند وقوع حادث سيبراني متوسط الشدة، وذلك خلال 8 ساعات كحد أقصى من تأكيد الحادث. (ملحق رقم 4) ج- تقديم تقرير الحالة، في حالة وجود تحديثات جديدة على الإخطار السابق (الوارد في أ،ب) حتى يتم حل الحادث/المشكلة نهائياً. (ملحق رقم 5) د- تقديم تقرير التعافي بعد حل الحادث واستئناف العمليات إلى وضعها الطبيعي. (ملحق رقم 6).
10.4	**تصنيف شدة الحوادث والإستجابة لها (Incident Severity Classification and Response)**
المبدأ	إعتماد تصنيف الحوادث السيبرانية وشدة تأثيرها كأساس لإدارة المخاطر السيبرانية، بما يتيح تحديد الأولويات في الإستجابة، وحماية الأصول والأنظمة الحيوية، وضمان استمرارية الأعمال.
الهدف	تمكين الجهة من تصنيف الحوادث السيبرانية وفق طبيعتها وشدة تأثيرها على الأنظمة الحيوية والعمليات والخدمات والسمعة، ضمان إستجابة سريعة وفعّالة.

الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	إنشاء نظام تصنيف للحوادث السيبرانية لتصنيف الحوادث وفقاً لطبيعة ونوع الحوادث وتأثيرها. يجب أن يشمل تصنيف الحوادث السيبرانية وصفاً شاملاً للحوادث كما يلي: أ- وصف نوع الحادث السيبراني (مثل: هجوم حجب الخدمة (DoS)، هجوم حجب الخدمة الموزع(DDoS) ، فيروس، دودة، تروجان، برمجيات خبيثة، اقتحام، اختراق، وصول غير مصرح به، تشويه موقع إلكتروني، سوء استخدام الأنظمة، الإستخدام غير المناسب، هجوم متقدم مستمر(APT)، هجوم يوم الصفر، التصيد الاحتيالي المتقدم (Spear phishing)، صيد الحيتان (whaling) ، التصيد (Phishing)، التهكير الاجتماعي، أو غيرها. ب- وصف فئة السبب الجذري (مثل: فشل الأنظمة، أخطاء بشرية، ظواهر طبيعية، أفعال خبيثة، أو فشل الطرف الثالث). ج- تقييم شدة الحوادث السيبرانية لمساعدة الجهة على تحديد التأثير المحتمل والمخاطر المرتبطة بالحادث من الناحية التقنية. يهدف مستوى الشدة أيضاً إلى توضيح مدى سرعة التعامل مع التهديد/الحادث وإلى من يجب تصعيده. د- تصنيف أثر الحوادث بناءً على شدة تأثيرها (ملحق رقم 2)، وذلك على النحو التالي: i. يكون تصنيف الحادث مرتفع الشدة، في حال: a. فقدت الجهة القدرة على تقديم الخدمات الأساسية لـ(71%-100%) من قاعدة العملاء.. b. تم الوصول إلى بيانات حساسة أو تعديلها أو تسريبها، مما أثر على أكثر من 3% من قاعدة العملاء. c. تم الوصول إلى بيانات ذات تأثير مرتفع على الأعمال أو تم تعديلها. d. أن الأثر المالي الناتج عن الاحتيال أو سرقة الممتلكات أعلى بكثير مما يمكن للجهة امتصاصه.

	e. أن التعافي من الحادث غير ممكن (مثل: تسريب معلومات التعريف الشخصية ونشرها علناً). ii. يكون تصنيف الحادث متوسط الشدة، في حال: a. فقدت الجهة القدرة على تقديم الخدمات الأساسية لـ(50%-70%) من قاعدة العملاء. b. تم الوصول إلى بيانات حساسة أو تعديلها أو تسريبها، مما أثر على أقل من 3% من قاعدة العملاء. c. تم الوصل إلى بيانات ذات تأثير منخفض على الأعمال أو تم تعديلها. d. أن الأثر المالي الناتج عن الإحتيال أو سرقة الممتلكات أعلى قليلاً مما يمكن للجهة امتصاصه. e. أن الوقت اللازم للإسترداد غير متوقع، حيث يتطلب الأمر وجود موارد إضافية أو مساعدة خارجية. iii. يكون تصنيف الحادث منخفض الشدة، في حال: a. لا يزال بإمكان الجهة تقديم الخدمات الأساسية لجميع العملاء ولكن بكفاءة أقل. b. فقدت الجهة القدرة على تقديم الخدمات الأساسية لأقل من(50%) من قاعدة العملاء. c. تم الوصول للبيانات الحساسة ولكن لم يتم تعديلها أو تسريبها. d. تم الوصول إلى بيانات غير مصنفة أو تم تعديلها. e. أنه يمكن للجهة امتصاص الأثر المالي الناتج عن الإحتيال أو سرقة الممتلكات. f. إمكانية توقع الوقت اللازم للتعافي.
10.5	**خطة استمرارية الأعمال التعافي من الكوارث (Business Continuity and (Disaster Plan**
10.5.1	**خطة استمرارية الأعمال (Business Continuity Plan)**
المبدأ	التعافي في حالة وقوع كارثة وإعادة تشغيل العمليات/ الأعمال بصورة طبيعية بأقل قدر ممكن من الخسائر المالية والمتعلقة بالسمعة.

الهدف	إعتماد عملاً متكاملاً لإستمرارية الأعمال يضمن القدرة علي التعافي بسرعة واستئناف العمليات المهمه في جميع الظروف الطارئة، مع تعزيز جاهزية جميع أصحاب المصلحة واستقرار العمليات.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن يكون لدى الجهه خطة معتمدة لإستمرارية الأعمال تتناول التعافي من الكوارث لمواصلة عملها.
(2)	تعميم خطة استمرارية الأعمال المعتمدة على جميع أصحاب المصلحة المعنيين، ويتلقى الجميع نسخة من الخطة المعدلة كلما حدث أي تعديل أو تغيير.
(3)	الإحتفاظ بالوثائق المتعلقة بخطة استمرارية الأعمال في مكان آمن خارج الموقع الرئيسي والموقع البديل، والإحتفاظ بنسخة واحدة في المكتب للرجوع إليها.
(4)	تنسيق خطة استمرارية الأعمال وإسنادها من خلال تحليل تأثير الأعمال (BIA) وخطة التعافي من الكوارث مع الأخذ في الإعتبار متطلبات النظام والعمليات والترابطات.
(5)	أن تتناول خطة استمرارية الأعمال ما يلي: أ- خطة العمل لإستعادة العمليات والأعمال. ب- جهات الإتصال في حالات الطوارئ وعناوين وأرقام هواتف الموظفين وموردي ومزودي الخدمات والوكلاء. ج- قائمة بالعناصر مثل :النسخ الإحتياطية وأجهزة الحاسوب المحمولة ووسائط التخزين المحمولة وما إلى ذلك.
(6)	اختبار خطة استمرارية الأعمال وخطة التعافي من الكوارث ومراجعتها مرة واحدة على الأقل سنوياً لضمان فعاليتها.
10.5.2	**خطة التعافي من الكوارث (Disaster Recovery Plan)**
المبدأ	إعتماد خطة للتعافي من الكوارث بما يضمن استعادة الأنظمة المهمة والعمليات الأساسية بسرعة وكفاءة، مع تعزيز جاهزية الموظفين وضمان استمرارية الأعمال في جميع الظروف الطارئة.
الهدف	ضمان قدرة الجهة على استعادة الأنظمة المهمة والعمليات الأساسية بسرعة وكفاءة عند وقوع الكوارث أو الأعطال الحرجة، مع حماية الأصول والمعلومات وتقليل الأثر المالي والتشغيلي ، وتعزيز استقرار الأعمال وثقة الجمهور.

الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أن يكون لدى الجهة خطة معتمدة للتعافي من الكوارث. ويجب عند صياغة وإنشاء خطة التعافي السريع من الكوارث أن تتضمن تحليل السيناريوهات لتحديد ومعالجة أنواع مختلفة من سيناريوهات الطوارئ. مع الاخذ في الإعتبار سيناريوهات مثل الإنقطاعات الرئيسية للنظام والتي قد تكون ناجمة عن أعطال في النظام أو أعطال في الأجهزة أو أخطاء في التشغيل أو حوادث أمنية بالإضافة إلى التوقف التام في مركز البيانات الرئيسي.
(2)	إنشاء موقع للتعافي من الكوارث (DRS) منفصل جغرافياً عن الموقع الرئيسي لتمكين استعادة الأنظمة الحيوية واستئناف العمليات والاعمال عند حدوث عطل في الموقع الرئيسي.
(3)	إذا لم يكن موقع التعافي من الكوارث (DRS) منفصلًا جغرافياً بشكل صحيح، يمكن للجهة إنشاء موقع ثالث في منطقة مختلفة يتم التعامل معه كموقع للتعافي من الكوارث (DRS) بعيد عن الموقع الرئيسي. في مثل هذه الحالة، سيتم التعامل مع (DRS) في موقع قريب على أنه موقع التعافي من الكوارث القريب ويجب تهيئته وفقاً لذلك.
(4)	أن يكون موقع التعافي من الكوارث ومركز البيانات (الموقع القريب) مجهزاً بأجهزة ومعدات اتصالات متوافقة لدعم الخدمات الحيوية لعمليات الأعمال في حالة وقوع كارثة.
(5)	الحفاظ على الأمن المادي والبيئي لأنظمة موقع التعافي من الكوارث ومركز البيانات (الموقع القريب).
(6)	تحديد أولويات استعادة النظام واستئناف الأعمال ووضع أهداف محددة لإستعادة القدرة على العمل بما في ذلك هدف وقت الإستعادة (RTO) وهدف نقطة الإستعادة (RPO) لأنظمة وتطبيقات تقنية المعلومات. هدف وقت الاستعادة (RTO) هو المدة الزمنية من نقطة التعطل، التي يجب استعادة النظام خلالها. وهدف نقطة الاستعادة يشير إلى المقدار المقبول من فقدان البيانات لنظام تقنية المعلومات أثناء حدوث كارثة.
(7)	أن تأخذ في الاعتبار أوجه الترابط بين الأنظمة الحرجة عند وضع خطة التعافي وإجراء اختبارات الطوارئ.
(8)	يمكن للجهة وضع استراتيجيات وتقنيات الاستعادة مثل التوافرية في الموقع ونسخ البيانات في الوقت الفعلي لتعزيز قدرة الجهه على لاستعادة.
(9)	الحفاظ على أمن المعلومات بشكل صحيح طوال عملية التعافي.

(10)	الاحتفاظ بنسخة محدثة ومختبرة من خطة التعافي من الكوارث بشكل آمن خارج الموقع الرئيسي/الموقع البديل بالإضافة إلى الموقع الرئيسي/موقع الإنتاج، كما يجب الاحتفاظ بنسخة واحدة في المكتب للرجوع إليها.
(11)	باختبار كفاءة متطلبات التعافي من الكوارث والتحقق من فعاليتها وقدرة الموظفين على تنفيذ إجراءات الطوارئ والتعافي اللازمة على الأقل سنوياً.
(12)	إشراك موظفيها في تصميم وتنفيذ حالات اختبار شاملة للتحقق من أن الأنظمة المستعادة تعمل بشكل صحيح.
(13)	أن تشتمل وثائق اختبار التعافي من الكوارث كحد أدنى على النطاق والخطة ونتائج الاختبار ويجب إرسال تقرير الاختبار إلى الإدارة وأصحاب المصلحة الآخرين والإحتفاظ به للضرورة المستقبلية.
10.6	**إدارة النسخ الإحتياطية للبيانات واستعادتها (Data Backup and Recovery Management)**
المبدأ	وجود خطة عمل متكاملة لإدارة النسخ الاحتياطية واستعادة البيانات بما يضمن حماية المعلومات المهمة، واستمرارية الأعمال، مع تأمين النسخ الاحتياطية وتشغيلها بفعالية عند الحاجة، والحفاظ على سرية وسلامة وتوافر البيانات.
الهدف	ضمان حماية واستعادة البيانات المهمة بسرعة وكفاءة عند فقدانها أو حدوث أعطال، من خلال تنفيذ نسخ احتياطية مخططة ومؤمنة مع ضمان مراقبتها بشكل مستمر، واختبار قدرتها على الاسترجاع بانتظام لدعم استمرارية الأعمال والإلتزام بالمتطلبات القانونية والتنظيمية.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	وضع سياسة للنسخ الإحتياطية واستعادة البيانات.
(2)	أن يكون لكل تطبيق من تطبيقات الأعمال استراتيجية نسخ احتياطي مخططة مسبقاً ومجدولة وموثقة، والتي تتضمن عمل نسخ احتياطية آنية وغير آنية ، ونقل النسخ الإحتياطية لتأمين التخزين خارج الموقع.
(3)	إنشاء جدول النسخ الإحتياطي المخطط له مسبقاً مفصلًا لكل تطبيق عمل بما يتوافق مع تصنيف التطبيق والمعلومات التي يدعمها ويجب أن يحدد نوع النسخ الإحتياطي المطلوب

	(Incremental, Differential, Partial, or Full) مع المراقبة في الوقت الحقيقي لكل تفاصيل جدول النسخ الإحتياطي.
(4)	تحديد تكرار النسخ الإحتياطية للمعلومات بما يتوافق مع تصنيف المعلومات ومتطلبات خطط استمرارية الأعمال لكل تطبيق.
(5)	أن تتضمن تفاصيل جدول النسخ الإحتياطي المخطط له مسبقاً لكل تطبيق عمل فترة الإحتفاظ بالمعلومات التي تم نسخها احتياطياً أو أرشفتها، ويجب أن تكون فترة الإحتفاظ متسقة مع المتطلبات القانونية والتنظيمية المحلية.
(6)	أن تكون جميع الوسائط التي تحتوي على معلومات احتياطية معنونة بمحتوى المعلومات ودورة النسخ الإحتياطي والمعرف التسلسلي للنسخ الإحتياطي وتاريخ النسخ الإحتياطي.
(7)	الإحتفاظ بوثائق جرد النسخ الإحتياطية وسجلاتها، والتحقق منها وتوقيعها من قبل المسؤول.
(8)	على الجهة تشفير البيانات الإحتياطية في ووحدات/ وسائط التخزين التي تحتوي على معلومات حساسة أو سرية قبل نقلها خارج الموقع للتخزين.
(9)	الإحتفاظ بنسخة واحدة على الأقل من النسخ الإحتياطية في الموقع لوقت التسليم الحرج.
(10)	توثيق عملية استعادة المعلومات من كل من التخزين الإحتياطي في الموقع وخارج الموقع.
(11)	أن تقوم الجهه بإجراء اختبار دوري والتحقق من قدرة استرجاع عمليات النسخ الاحتياطية وتقييم ما إذا كانت كافية وفعالة بما فيه الكفاية لدعم عملية استرجاع المعلومات في الجهه.

11. الأمن السيبراني للطرف الثالث (Third Party Cybersecurity)

11.1	إدارة العقود والمقاولين والموردين (Contractors and Vendors Management)
المبدأ	وضع وتنفيذ عمليات لتحديد، توقع ،تنفيذ،مراقبة، تقييم، إدارة، وتخفيف المخاطر السيبرانية ضمن إدارة العقود والموردين.
الهدف	ضمان تضمين متطلبات الأمن السيبراني التي تم الإتفاق عليها في العقد قبل توقيعه بفعالية من قِبل الموردين، وضمان الإلتزام بتلك المتطلبات من خلال المراقبة والتقييم المنتظم خلال فترة العقد.

الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	تحديد واعتماد وتطبيق متطلبات إدارة المخاطر السيبرانية ضمن عمليات إدارة العقود والموردين، وتشمل ما يلي: أ- ضمان دعم متطلبات مرونة الأمن السيبراني بالشكل الكافي. ب- التنبؤ وتقييم المخاطر السيبرانية المتعلقة بالأنشطة المتعاقد عليها. ج- تقييم الموردين وإشراك وظيفة الأمن السيبراني في التقييم، ومراقبة تنفيذ العقود. د- تخصيص ضوابط الأمان السيبراني وفقاً لمستوى المخاطر وتعقيد العلاقة مع المورد. هـ- التأكد من أن الخدمات المقدمة من الموردين تطابق -على الأقل- نفس مستوى المرونة المطلوبة اذا تم تنفيذها داخلياً.
(2)	تنفيذ اجراءات فحص مناسبة لاختيار الموردين ،وأن تشمل اجراءات الفحص: أ- مراجعة الخلفية التجارية. ب- السمعة. ج- الاستراتيجية. د- مدى الإلتزام باللوائح التنظيمية. هـ- الأداء والوضع المالي. و- فعالية برنامج أمن المعلومات (بما في ذلك العمليات والضوابط الداخلية). ز- العمليات والتقنيات المستخدمة لدعم النشاط المتعاقد عليه . ح- خطط التعافي من الكوارث (DR) وخطط استمرارية الأعمال (BCP)،وخطط التكنولوجيا والتكرار. ط- آليات الإبلاغ عن الحوادث وإدارتها.
(3)	أن توضح الإتفاقية التعاقدية مع الطرف الثالث (المقاولين والموردين) حقوق ومسؤوليات كل طرف فيما يتعلق بإدارة مخاطر الأمن السيبراني، ويجب أن تشمل العقود ما يلي: أ- نطاق وطبيعة الأنشطة التي سيقوم بها المورد. ب- تعريف جميع أنواع البيانات، لا سيما ما يُعد "معلومات سرية"، وبيان ملكيتها وطريقة الوصول إليها.

	ج- دور المورد في حماية البيانات التي يتم مشاركتها من المخاطر السيبرانية، بما في ذلك البيانات المقدمة لطرف ثالث كمقاول فرعي أو مدقق. د- مسؤوليات المورد في الإلتزام للمتطلبات القانونية والتنظيمية المتعلقة بحماية البيانات وعدم الكشف عن البيانات الشخصية.
(4)	إعداد خطة إستجابة واضحة للحوادث السيبرانية تتضمن: أ- الإطار الزمني لإخطار المورد. ب- الإجراءات المتخذة لضمان وقف الاختراق. ج- طريقة التحقيق والإبلاغ عن النتائج. د- تحديد المعلومات التي تم اختراقها. هـ- خطوات التخفيف لمنع أي خرق أو تسلل مستقبلي.
(5)	على كل طرف تنفيذ التزامات الأمن السيبراني المتفق عليها مثل تقييم المخاطر، مراقبة النظام، تقييم الأداء، المراجعة، والتقارير الدورية.
(6)	تحديد الإجراءات المتبعة في حال حدوث خرق أمني.
(7)	تحديد مسؤوليات كل طرف فيما يتعلق بالإلتزام لتدابير الأمن السيبراني في حالة إنهاء أو تجديد العقد.
(8)	الحق في تنفيذ عمليات تدقيق ومراجعة أمنية سيبرانية بشكل دوري.
(9)	أن يتم اختبار وتحديث تدابير الأمن السيبراني في الاتفاقية التعاقدية بشكل دوري.
(10)	ضمان وجود عملية واضحة للتحقق من التزام المورد لمتطلبات الأمن السيبراني للجهة.
(11)	التأكد من حماية أنظمة البريد والرسائل، بما في ذلك الأنظمة المستخدمة من قِبل المقاولين والموردين.
11.2	**الحوسبة السحابية (Cloud computing)**
المبدأ	وضع وتنفيذ العمليات اللازمة لتحديد وتقييم وتوقّع وإدارة وتخفيف مخاطر الأمن السيبراني ضمن سياسات وإجراءات الحوسبة السحابية ويجب تقييم فعاليتها دورياً.
الهدف	ضمان أن تكون متطلبات الأمن السيبراني المُتفق عليها من قبل الجهة معالجة بشكل كافٍ ضمن ترتيبات الخدمات السحابية مع الأطراف الثالثة.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	وضع سياسة شاملة للحوسبة السحابية تشمل الهيكل التنظيمي، الإجراءات، والعمليات لضمان إدارة مخاطر الأمن السيبراني.
(2)	مواءمة السياسة مع استراتيجية وأهداف الجهة في تكنولوجيا المعلومات، بما في ذلك شهية المخاطرة (Risk appetite).
(3)	مراجعة سياسة الحوسبة السحابية بشكل دوري لضمان التوافق مع متطلبات الأمن السيبراني وأن تدعم هذه المتطلبات مرونة نظام الأمن السيبراني.
(4)	ممارسة الرقابة من الإدارة العليا على العمليات اليومية وإدارة المخاطر المتعلقة بالأمن السيبراني.
(5)	التنبؤ وتقييم جميع المخاطر المرتبطة باستخدام خدمات الحوسبة السحابية من مزودي الخدمات السحابية (CSPs) من أطراف ثالثة، وضمان أن تكون إدارة المخاطر والمراقبة والتحكم متناسبة مع مدى أهمية/حجم الاتفاق.
(6)	إجراء العناية الواجبة المناسبة (Due Diligence) ويشمل ما يلي: أ- اعتماد/ترخيص المزود. ب- قدرات خدمات تكنولوجيا المعلومات. ج- سجل الأداء السابق. د- هيكل إدارة المخاطر. هـ- فعالية إطار الأمن السيبراني بما في ذلك اختبارات الثغرات. و- عمليات المصادقة والتحكم. ز- الضوابط الداخلية . ح- الإلتزام بمعايير الصناعة. ط- متطلبات حماية البيانات والتشفير،والتوافق مع الممارسات والمعايير العالمية.
(7)	مراجعة الإتفاقيات مع مزوّدي خدمات الحوسبة السحابية بشكل دوري لضمان عدم وجود تأثير سلبي على أمن المعلومات السيبرانية للجهة.
(8)	الحصول على موافقة مسبقة من بنك السودان المركزي قبل الدخول في أي ترتيبات سحابية جوهرية مع مزوّدي خدمات سحابية عالميين، مع تقديم التفاصيل التالية: أ- نطاق خدمات الحوسبة السحابية التي سيتم الحصول عليها. ب- نوع وتصنيف البيانات التي ستُخزن على السحابة.

	ج- تفاصيل تقييم المخاطر والنتائج المستخلصة. د- التاريخ المقترح لبدء التنفيذ وفترة التعاقد. هـ- تفاصيل مزوّد الخدمة السحابية (CSP). و- موقع تخزين البيانات. ز- الدعم التشغيلي المقدّم من مزوّد الخدمة. ح- ضوابط الأمان الأساسية التي يحددها المزود. ط- هيكل الحوكمة والمراقبة بما يشمل التدابير الأمنية المقترحة من الجهة. ي- استراتيجيات وإجراءات إدارة التغيير. ك- الترتيبات الخاصة بمراجعة مزوّد الخدمة من قبل مدققي حسابات الجهة والبنك المركزي. ل- تفاصيل إدارة استمرارية الأعمال (BCM) واستراتيجية الخروج.
(9)	التأكد من الإلتزام بالضوابط الأمنية في جميع ترتيبات الخدمات السحابية الجوهرية وغير الجوهرية، وعدم التعاقد من الباطن مع مزوّد خدمة عالمي بدون موافقة مسبقة من بنك السودان المركزي.
(10)	التأكد من أن مزوّدي الخدمات السحابية يلتزمون بالآتي: أ- معايير حماية قوية تشمل معايير أمنية صارمة. ب- إجراءات إدارة مخاطر الأمن السيبراني، سياسات إدارة الوصول إلى البيانات. ج- اتفاقيات ملزمة تتماشى مع متطلبات بنك السودان المركزي والمتطلبات القانونية الأخرى.
(11)	التأكد من أن مزودي خدمات الحوسبة السحابية يحافظون على سرية البيانات والمعلومات الخاصة بالجهات، ويقيدون استخدام هذه البيانات فقط للأغراض المتفق عليها.
(12)	توثيق الإتفاقيات المبرمة مع مزوّدي الخدمات السحابية، وأن تتضمن على الأقل المتطلبات الأمنية التالية: أ- أن تكون البيانات والمعلومات في السحابة منفصلة منطقياً وتشغيلياً عن بيانات الجهات الأخرى التي يستضيفها مزود الخدمة، باستخدام ضوابط وصول مناسبة وأمن بيانات، بما يتماشى مع المعايير الدولية.

	ب- التأكد من قدرة مزوّد الخدمة على تمييز المعلومات والخدمات الخاصة بالجهة وفصلها عن غيرها من الجهات الأخرى. ج- تطبيق تشفير شامل للبيانات الحساسة (End-to-End Encryption)، مع إمكانية تطبيق تشفير مزدوج حسب تقييم المخاطر. د- فرض رقابة صارمة على عمليات التشفير، بما في ذلك استخدام سياسات إدارة مفاتيح التشفير القوية، والإجراءات المتعلقة بإنشاء وتوزيع وتحديث وإلغاء المفاتيح. هـ- أن تظل مفاتيح التشفير وأدوات المصادقة الأخرى تحت سيطرة الجهات ، وتُخزّن في وحدة أمان الأجهزة (HSM) في الحالات الإستثنائية التي يتم فيها الإحتفاظ بالمفاتيح لدى مزود الخدمة، يجب أن تخضع لرقابة صارمة وإجراءات حماية. و- ضمان حقوق الملكية الحصرية للجهات على بياناتها. ز- على مزوّد الخدمة إخطار الجهة بأي خرق أمني أو تسريب بيانات، بما في ذلك الإجراءات التصحيحية المتخذة. ح- تقييد استخدام البيانات المتبقية مثل سجلات الوصول لاستخدامها فقط في الأغراض المتفق عليها. ط- تنفيذ خطة إدارة استمرارية الأعمال (BCM) لكل ترتيبات الحوسبة السحابية، وضمان إخطار الجهة على الفور بأي حوادث قد تؤثر على فقدان البيانات أو تعطل الخدمات.
(13)	التأكد من وجود استراتيجية خروج قوية تشمل حق الجهة في استرجاع بياناتها، وضمان سهولة نقل البيانات أو الأنشطة، بالإضافة إلى الحذف النهائي للبيانات وأي أجهزة مخصصة إن وجدت.
(14)	التأكد من أن للجهة الحق في المراجعة والفحص في مواقع مزوّد الخدمة، بما يشمل التدقيق الأمني والتقارير الخاصة بمراجعات الطرف الثالث واختبارات الثغرات الأمنية (VA & PT).

11.3	الإستعانة بمصادر خارجية (Outsourcing)
المبدأ	وضع وتنفيذ العمليات اللازمة لتحديد، توقّع، تقييم، تخفيف، وإدارة مخاطر الأمن السيبراني المرتبطة بسياسة الاستعانة بمصادر خارجية والعمليات المتعلقة بها.
الهدف	ضمان أن المتطلبات المتفق عليها للأمن السيبراني من قبل الجهة يتم التعامل معها بشكل كافٍ ضمن ترتيبات الإستعانة بمصادر خارجية مع الطرف الثالث، وأن الإلتزام بتلك التدابير يخضع للرقابة والتقييم بشكل منتظم.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	وضع سياسة شاملة وواضحة للاستعانة بمصادر خارجية، يتم تعريفها واعتمادها وتنفيذها والتواصل بشأنها من قبل مجلس الإدارة. وأن تُحدد السياسة المسؤوليات العامة المتعلقة بالإلتزام، التدقيق، والبنية التحتية لإدارة المخاطر.
(2)	تنفيذ برنامج شامل لإدارة مخاطر الأمن السيبراني المرتبطة بالإستعانة بمصادر خارجية لمعالجة الأنشطة المُستعان بها والعلاقات مع مقدمي الخدمات.
(3)	الحصول على موافقة مسبقة محددة من بنك السودان المركزي قبل الإستعانة بمصادر خارجية لأي أنشطة متعلقة بالأمن السيبراني.
(4)	التأكد من أن متطلبات إدارة مخاطر الأمن السيبراني قد تم تحديدها، والموافقة عليها، تقييمها، تطبيقها، ومعالجتها ضمن السياسات وعمليات الاستعانة بمصادر خارجية.
(5)	التأكد من أن عملية إدارة مخاطر الأمن السيبراني تأخذ في الاعتبار تقييم المخاطر التالية: أ- المخاطر المتعلقة بالأنشطة المستعان بها خارجياً، والتي تشمل: i. حساسية البيانات التي يتم الوصول إليها أو حمايتها أو التحكم بها من قبل مزوّد الخدمة. ii. حجم المعاملات. iii. الأهمية بالنسبة لأعمال الجهة. ب- المخاطر المتعلقة بمزودي الخدمة، وتشمل: i. الوضع المالي. ii. استمرارية الأعمال. iii. القدرة على تقديم نظام معلومات إداري دقيق وملائم وفي الوقت المناسب.

	iv. الإعتماد على المقاولين من الباطن. v. التكرار والموثوقية في خطوط الاتصال. ج- المخاطر المتعلقة بالتكنولوجيا المستخدمة وتشمل الموثوقية، والأمن.
(6)	التأكد من أن الخدمات التى يتم إســنادها إلى جهات خارجية يتم التعامل معها على الأقل بنفس مستوى مرونة الأمن السيبراني المطلوب فيما لو تم تنفيذ تلك الخدمات داخلياً.
(7)	أن تطبق مستوى مناسب من العناية الواجبة عند اختيار أطراف ثالثة بغرض الاستعانة بمصادر خارجية، ويشمل ذلك تقييم ما يلي: أ- المؤهلات وكفاية الموارد. ب- الوضع المالي. ج- قدرة وكفاءة تقديم الخدمة والحالة العامة. د- بنية الأنظمة والتقنية. هـ- بيئة الرقابة الداخلية،وسجل الأمن، وتغطية التدقيق. و- الإلتزام القانوني والتنظيمي. ز- تغطية التأمين. ح- القدرة على تلبية متطلبات درء الكوارث واستمرارية الأعمال.
(8)	أن تصف العقود الخاصة بالاستعانة بمصادر خارجية جميع الأدوار والمسؤوليات وحقوق جميع الأطراف، وتشمل كحد أدنى العناصر التالية: أ- نطاق الخدمات. ب- تحديد ومراجعة الحد الأدنى لمستويات الخدمة والمتطلبات، والتدابير اللازمة لتلبية معايير الأمن السيبراني. ج- الأحكام المتعلقة بأمن وسرية معلومات الجهة والإبلاغ عن أي حوادث إلكترونية (مثل خروقات البيانات) والتقارير المطلوبة قانونياً. د- الضوابط الداخلية لمقدم الخدمة الخارجي. هـ- حقوق التدقيق. و- خطة استئناف الأعمال وخطة الطوارئ. ز- الاستعانة بمقاولين من الباطن ومزودي خدمات متعددين. ح- أحكام خاصة بعملية تسوية النزاعات. ط- أحكام التعويض عن الإهمال من قبل مقدم الخدمة.

	ي- تحديد مسؤولية مقدم الخدمة عن الأضرار. ك- بند إنهاء العقد. ل- أحكام تتعلق بالإخطار بأي تغييرات تتعلق بالتعاقد من الباطن.
(9)	أن تكون هناك عملية واضحة لضمان امتثال مزودي الخدمة الخارجيين لتدابير الأمن السيبراني المعتمدة من الجهة ، وتحقيق مستوى المرونة السيبرانية المطلوبة في ترتيبات الاستعانة بمصادر خارجية.
(10)	تقييم الحاجة الفعلية إلى الإستعانة بمصادر خارجية في العمليات الحرجة.
(11)	التحقق من مؤهلات مزودي الطرف الثالث عند تقييمهم وإدارتهم للأصول الحرجة للجهة.
(12)	أن ينص الاتفاق مع مزود الخدمة على حق التدقيق من قبل الجهة ، وكذلك حق التفتيش من قبل بنك السودان المركزي لإجراء التفتيش أو المراجعة.
(13)	للجهة الحق في إنهاء التعاقد واسترداد بياناتها عند الإنهاء وحذف بياناتها نهائياً وأن تكون غير قابلة للاسترجاع.

12. الإلتزام والمراجعة (Audit and Compliance)

12.1	الإلتزام بالمتطلبات التنظيمية (Compliance with Regulatory Requirements)
المبدأ	وضع عملية منهجية لتحديد الآثار التنظيمية ذات الصلة بالأمن السيبراني، التواصل بشأنها، وضمان الإلتزام بها.
الهدف	ضمان الإلتزام بالأنظمة واللوائح التي تؤثر على الأمن السيبراني في الجهة
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	ضمان الإلتزام بالقوانين، اللوائح، والضوابط ذات الصلة بالأمن السيبراني والخصوصية، إضافة إلى ما سيصدر لاحقاً عن بنك السودان المركزي والتشريعات الوطنية، بما في ذلك. على سبيل المثال لا الحصر. ما يلي: أ- قانون المعاملات الإلكترونية لسنة 2007. ب- قانون جرائم المعلوماتية لسنة 2019/2007 ج- لائحة تنظيم أعمال الدفع لسنة 2013.

	د- لائحة ترخيص وتنظيم أعمال الجهات للدفع عبر الموبايل لسنة 2020.
(2)	إنشـــاء عملية لضـــمان الإلتزام بالمتطلبات التنظيمية ذات الصـــلة وتأثيرها على الأمن السيبراني على مستوى الجهة ككل، وينبغي أن تتضمن هذه العملية مايلي: أ- تنفيذ المراجعة بشـكل دوري أو عند دخول متطلبات تنظيمية جديدة حيز التنفيذ. ب- إشراك ممثلين من الوحدات والمجالات الرئيسية داخل الجهة. ج- تحديث ســياســات الأمن الســيبراني ومعاييره وإجراءاته بما يواكب أي تغييرات تنظيمية.
12.2	**الإلتزام بمعايير الصناعة (المحلية والدولية) (Compliance with Industry (Standards "Local and International"**
المبدأ	الإلتزام بمعايير الصناعة، سواء كانت محلية أو دولية.
الهدف	ضمان الإلتزام بمعايير الصناعة المعتمدة على المستوى المحلي والدولي.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	أحدث الإصدارات من اللوائح والمعايير الدولية ذات الصلة بما في ذلك، على سبيل المثال لا الحصر: أ- معيار NIST-CSF. ب- معيارISO27001. ج- معيار SWIFT CSP لأمان عملاء سويفت. د- معيار PCI PTS لأجهزة إدخال الرقم السري في الدفع باستخدام البطاقات. هـ- معيار PCI PA-DSS لتطبيقات الدفع المطورة باستخدام البطاقات. و- معيار PCI DSS لأمان بيانات صناعة بطاقات الدفع. ز- المعيار الفني .EMV.(يوروباي، ماستركارد، وفيزا).
12.3	**مراجعة الأمن السيبراني (Cybersecurity Review)**
المبدأ	التحقق من أن ضوابط الأمن السيبراني مصممة ومطبقة بشكل آمن، وأن فعاليتها تخضع للرقابة والمتابعة المستمرة.

الهدف	وجود مجموعة واضحة من السياسات والإجراءات التي تنظم إجراء عملية مراجعة الأمن السيبراني بصورة شاملة، مستقلة، ومنتظمة، تُجرى وفقاً لمعايير المراجعة المعتمدة في السودان، وبما يتماشى مع إطار الأمن السيبراني الصادر عن بنك السودان المركزي.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	
(1)	المراجعة الداخلية: أ- اعتماد خطة تنفيذ مراجعة الأمن السيبراني من قبل مجلس الإدارة أو من يفوضه. ب- إجراء مراجعة داخلية للأمن السيبراني من قبل إدارة المراجعة الداخلية في الجهة. ج- أن يقوم بالمراجعة الداخلية موظفون يتمتعون بخبرة ومهارات كافية في مجال مراجعة الأمن السيبراني. د- أن تكون عملية مراجعة الأمن السيبراني جزءاً من برنامج مراجعة مستقل عن أي وظيفة قد تتعارض مع مهام البرنامج داخل الجهة، وتتحمل المراجعة الداخلية مسؤولية التأكد من: i. موثوقية عملية تحديد المخاطر السيبرانية، وتقييم آليات تقييم المخاطر، ومعالجة تلك المخاطر بما يتوافق مع نتائج عملية التقييم عبر جميع وحدات العمل. ii. مدى فعالية وكفاءة الضوابط الداخلية، إدارة المخاطر، ونظم الحوكمة، في ضوء كافة المخاطر السيبرانية الحالية والمتوقعة. iii. تنفيذ عملية التوثيق بشكل كامل، والتأكد من شمولية السياسات والمعايير والإجراءات والإرشادات المعتمدة، والتأكد من وجود الموافقات الرسمية وآليات التنفيذ الفعّالة. iv. موثوقية وكفاءة وسلامة أنظمة وعمليات المعلومات الإدارية. v. مدى الإلتزام بالقوانين واللوائح ذات الصلة. vi. توفر الضوابط الوقائية وعمليات المراقبة المناسبة. vii. مراجعة إجراءات إدارة الحوادث وتقييم كفاءة الإستجابة ومعالجة الحوادث.

	viii. تقديم تقارير دورية إلى مجلس الإدارة والإدارة العليا حول نتائج المراجعة وتقديم الخطة التصحيحية لها ، أو عند الطلب. ix. إجراء المراجعة السيبرانية المبنية على المخاطر بشكل سنوي على الأقل للمجالات عالية الخطورة، ومرة كل سنتين للمجالات متوسطة الخطورة، وكل ثلاث سنوات للمجالات منخفضة الخطورة . x. على مجلس الإدارة اعتماد تقرير المراجعة الداخلية واتخاذ التدابير المناسبة لمعالجة التوصيات الواردة فيه.
(2)	المراجعة الخارجية: أ- إدراج عملية مراجعة الأمن السيبراني ضمن برنامج المراجعة الخارجية بهدف التأكد من شمولية وفعالية برنامج الأمن السيبراني وآليات تنفيذه. ب- تنفيذ المراجعة الخارجية سنوياً على الأقل للخدمات الحرجة وذات التأثير العالي على الأعمال، ويمكن إدراج باقي الخدمات ضمن خطة مراجعة دورية تمتد لثلاث سنوات. ج- أن يكون المراجع الخارجي مستقلاً ومؤهلاً وذو خبرة في مجال الأمن السيبراني ومعتمد من قبل بنك السودان المركزي. د- تغيير المراجعين الخارجيين المسؤولين عن مراجعة الأمن السيبراني كل ثلاث سنوات كحد أقصى. هـ- إطلاع مجلس الإدارة والإدارة التنفيذية بشكل منتظم أو عند الطلب على نتائج المراجعة الخارجية والتوصيات المصاحبة لها.

13. التعاون (Collaboration)

13.1	مشاركة المعلومات (Information Sharing)
المبدأ	التعاون وتبادل المعلومات بين الجهات الداخلية والخارجية لتحسين المهارات وتبادل المعرفة والقيادة.
الهدف	ضمان التعاون الوثيق وتبادل المعلومات لتمكين القطاع المصرفي والمالي من مواجهة التهديدات السيبرانية المتطورة.

الضوابط	
يجب على الجهات الإلتزام بالآتي:	
(1)	تكوين فرق/ مجموعات عمل بغرض التعاون وتبادل المعلومات.
(2)	يمكن لفرق العمل /المجموعات القيام بالأنشطة التالية: أ- وضع بروتوكولات تعاون واضحة للتنسيق بين الفرق الأمنية في القطاع والجهات الرقابية عند وقوع حادث كبير مشترك، لضمان اتخاذ إجراءات احتواء موحدة. ب- تبادل المعلومات حول الحوادث والتهديدات ونقاط الضعف المكتشفة داخل القطاع حتي يصبح أكثر مرونة في مواجهة الحوادث السيبرانية. ج- عقد منتديات لتبادل المعلومات والمعرفة للمساعدة على إدارة مخاطر الأمن السيبراني بشكل أفضل. د- تبادل المعلومات حول أحدث اتجاهات وتقنيات الأمن السيبراني التي تؤثر على القطاع المصرفي. هـ- تقديم الدعم والتوجيه بشأن مبادرات الأمن السيبراني والمساعدة في الإلتزام بالمعايير. و- إنشاء منصة لإثراء المبادرات الاستراتيجية ذات الصلة بمخاطر الأمن السيبراني وتنفيذها. ز- تيسير تحليل ومراقبة الضمانات والإجراءات اللازمة للإستجابة للحوادث السيبرانية. ح- التنسيق مع الجهات ذات الصلة بمجال الأمن السيبراني . ط- دعم مبادرات المرونة السيبرانية للحماية من الأحداث السيبرانية الضارة. ي- تبادل المعلومات السيبرانية التي يتم استيرادها تلقائيًا من مصادر موثوقة مختلفة. ك- تبادل المعلومات حول تكتيكات وميول المهاجمين (TTPs) وكيفية عمل القراصنة والأساليب المستخدمة. ل- إتاحة المعلومات المُحدثة حول حوادث الأمن السيبراني المكتشفة.

13.2	التوعية القطاعية (Sectoral Awareness)
المبدأ	أن يكون الأمن السيبراني جزءاً من ثقافة القطاع المصرفي والمؤسسات المالية، وليس مجرد مسؤولية تقنية.
الهدف	ضمان قيام حملات توعوية وإرشادية لتقوية الأمن السيبراني وممارسات تبادل المعلومات بشكل فعال في القطاع.
الضوابط	
يجب علي الجهات التعاون بينها لتنظيم دورات توعوية وإرشادية علي النحو التالي:	
(1)	التعاون بين مديري الأمن السيبراني والمسؤولين وأطراف ثالثة مؤهلة لإدارة وإعداد المواد التوعوية.
(2)	قيام دورات وحملات توعية تخص الأمن السيبراني وإشراك الجهات الاخري.
(3)	التحول والتفكير من ثقافة الإلتزام إلى ثقافة المسؤولية.
(4)	تنظيم جلسات توعوية وتدريبية مخصصة لمستويات وأدوار مختلفة للموظفين.
(5)	إصدار نشرات توعوية دورية عن أحدث التهديدات وأساليب الحماية، وإرسال تنبيهات عاجلة في حال اكتشاف هجوم واسع النطاق.
(6)	عقد ورش عمل لتبادل الخبرات بين مسؤولي الأمن السيبراني ، والتنسيق لإجراء تمارين محاكاة لهجمات سيبرانية لإختبار خطط الإستجابة ودرجة التعاون.

14. التقييم (Assessment)

14.1	التقييم الذاتي (Self-Assessment)
المبدأ	تقييم مستوى نضج ضوابط الأمن السيبراني في مواجهة التهديدات السيبرانية المتطورة.
الهدف	ضمان إجراء عملية تقييم وتحليل للفجوات، ومن ثم وضع خطط المعالجة وتحديد أولوياتها وتنفيذها ضمن الأطر الزمنية المسموح بها.
الضوابط	
يجب على الجهة الإلتزام بالآتي:	

(1)	أن يخضع تطبيق الإطار في الجهة لتقييم ذاتي دوري، وسيراجع بنك السودان المركزي التقييمات الذاتية لتحديد مستوى الإلتزام بالاطار ومستوى نضج الجهة في مجال الأمن السيبراني.
(2)	إعداد وتصنيف عملية التقييم الذاتي بناءً على تقييم ملف المخاطر الخاص بها. ويعتمد تقييم ملف المخاطر على قياس مستويات المخاطر استنادا على نوع وحجم وتعقيد العمليات ضمن الأنشطة والخدمات المُصنَّفة على سبيل المثال لا الحصر المجالات التالية: أ- قنوات تقديم الخدمة. ب- خدمات الإنترنت والخدمات المصرفية عبر الهاتف المحمول. ج- التقنيات والاتصالات. د- التهديدات الخارجية. هـ- الخصائص التنظيمية.
(3)	أن يتم التحكم ووضع المعالجات نتيجةً لتقييم ملف مخاطر الجهة وتقييم مستوى النضج في كل مجال.
(4)	وضع خطة تقييم لقياس فعالية وكفاءة الضوابط المُعتمدة في سيناريوهات واقعية، لضمان تحقيق الأهداف المتوقعة.

الملاحق

ملحق رقم (1): متطلبات الإخطار من الجهات إلى بنك السودان المركزي:

الجدول أدناه يوضح متطلبات الإخطار المتعلقة بالحوادث المصنفة حسب شدة الأثر (منخفضة، متوسطة، ومرتفعة)، استناداً إلى التأثيرات المعروفة والمتوقعة.

متطلبات الإخطار من الجهة إلى بنك السودان المركزي			
التأثير المعروف والمتوقع	الإخطار الأولي	تقرير الحالة	تقرير التعافي
منخفض	غير مطبق	غير مطبق	ربع سنوي
متوسط	خلال 8 ساعات من تأكيد الحادثة (ساعات يوم العمل فقط)	مرة كل يومي عمل	عند التعافي
مرتفع	خلال 4 ساعات من تأكيد الحادثة (سواء خلال ساعات يوم العمل أو خارجها)	مرة واحدة يومياً	عند التعافي

ملحق رقم (2) : مصفوفة تصنيف شدة تأثير الحادث

يجب على الجهة استخدام المعلومات الموضحة في الجدول أدناه، لاستيفاء متطلبات الملحق رقم (1):

أثر الحادث / مستوى الشدة	التأثير الوظيفي Functional impact	التأثير على المعلومات Information Impact			أثر التعافي Recoverability Impact
	انقطاع الخدمة Service Disruption	خرق خصوصية البيانات Data Privacy Breach	خرق سلامة البيانات Data Integrity Breach	خرق الممتلكات Proprietary Breach	
منخفض	فقدت الجهة القدرة على تقديم الخدمات الأساسية لأقل من(50%) من قاعدة العملاء.	تم الوصول للبيانات الحساسة ولكن لم يتم تعديلها أو تسريبها.	تم الوصول إلى بيانات غير مصنفة أو تم تعديلها.	يمكن للجهة امتصاص الأثر المالي الناتج عن الاحتيال أو سرقة الممتلكات.	الوقت اللازم للتعافي متوقع.
متوسط	فقدت الجهة القدرة على تقديم الخدمات الأساسية لـ(50%-70%) من قاعدة العملاء.	تم الوصول إلى بيانات حساسة أو تعديلها أو تسريبها، مما أثر على أقل من 3% من قاعدة العملاء.	تم الوصل إلى بيانات ذات تأثير منخفض على الأعمال أو تم تعديلها.	الأثر المالي الناتج عن الاحتيال أو سرقة الممتلكات أعلى قليلاً مما يمكن للجهة امتصاصه.	الوقت اللازم للاسترداد غير متوقع، حيث يتطلب الأمر إلى وجود موارد إضافية أو مساعدة خارجية.
مرتفع	فقدت الجهة القدرة على تقديم الخدمات الأساسية لـ(71%-100%) من قاعدة العملاء.	تم الوصول إلى بيانات حساسة أو تعديلها أو تسريبها، مما أثر على أكثر من 3% من قاعدة العملاء.	تم الوصول إلى بيانات ذات تأثير مرتفع على الأعمال أو تم تعديلها.	الأثر المالي الناتج عن الاحتيال أو سرقة الممتلكات أعلى بكثير مما يمكن للجهة امتصاصه.	التعافي من الحادث غير ممكن (مثل: تسريب معلومات التعريف الشخصية ونشرها علناً).

ملحق رقم (3) : مصفوفة شدة الأثر على القطاع

1- تصنيف شدة الأثر على القطاع يتم من قبل بنك السودان المركزي لتحديد النقطة التي يجب عندها تنسيق إستجابة موحدة لاحتواء الحادث والتعافي منه، وذلك على النحو التالي:

- يقوم بنك السودان المركزي بمراقبة الحوادث منخفضة الشدة على القطاع، دون تنسيق إجراء موحد ما لم تطالب إحدى الجهات بذلك.
- يقوم بنك السودان المركزي بإدارة إجراءات الإستجابة للحوادث متوسطة ومرتفعة الشدة على القطاع، لاحتواءها والتعافي منها.

2- سيستخدم بنك السودان المركزي المصفوفة التالية والتي توضح شدة الأثر على القطاع:

أثر الحادث / مستوى الشدة	التأثير الوظيفي Functional impact		التأثير على المعلومات Information Impact	
	انقطاع الخدمة Service Disruption	خرق خصوصية البيانات Data Privacy Breach	خرق سلامة البيانات Data Integrity Breach	خرق الممتلكات Proprietary Breach
منخفض	جهة واحدة لديها حادث مرتفع الشدة. أو 1 إلى 9 جهات لديها حادث متوسط الشدة. أو 1 إلى 15 جهة لديها حادث منخفض الشدة.	جهة واحدة لديها حادث مرتفع الشدة. أو 1 إلى 3 جهات لديها حادث متوسط الشدة. أو 1 إلى 10 جهات لديها حادث منخفض الشدة.	جهة واحدة لديها حادث مرتفع الشدة. أو 1 إلى 12 جهة لديها حادث متوسط الشدة أو 1 إلى 18 جهة لديها حادث منخفض الشدة.	جهة واحدة لديها حادث مرتفع الشدة. أو 1 إلى 3 جهات لديها حادث متوسط الشدة. أو 1 إلى 10 جهات لديها حادث منخفض الشدة.
متوسط	جهتين لديهما حادث مرتفع الشدة . أو 10 إلى 15 جهة لديها حادث متوسط الشدة. أو 16 إلى 22 جهة لديها حادث منخفض الشدة.	4 إلى 5 جهات لديها حادث متوسط الشدة . أو أكثر من 10 جهات لديها حادث منخفض الشدة . أو يؤثر على 3% إلى 10% من مستهلكي الخدمات المالية.	جهتين لديهما حادث مرتفع الشدة. أو 12 إلى 20 جهة لديها حادث متوسط الشدة. أو 19 إلى 24 جهة لديها حادث منخفض الشدة.	4 إلى 5 جهات لديها حادث متوسط الشدة . أو أكثر من 10 جهات لديها حادث منخفض الشدة. أو إجمالي الأثر المالي للاحتيال أو سرقة الممتلكات يفوق 3.5 مليار جنيه سوداني.

أثر الحادث / مستوى الشدة	التأثير الوظيفي Functional impact		التأثير على المعلومات Information Impact	
	انقطاع الخدمة Service Disruption	خرق خصوصية البيانات Data Privacy Breach	خرق سلامة البيانات Data Integrity Breach	خرق الممتلكات Proprietary Breach
مرتفع	أكثر من جهتين لديها حادث مرتفع الشدة. **أو** أكثر من 10 جهات لديها حادث متوسط الشدة. **أو** أكثر من 22 جهة لديها حادث منخفض الشدة.	جهتين أو أكثر لديها حادث مرتفع الشدة. **أو** أكثر من 5 جهات لديها حادث متوسط الشدة. **أو** يؤثر على أكثر من 10% من مستهلكي الخدمات المالية.	أكثر من جهتين لديها حادث مرتفع الشدة. **أو** أكثر من 20 جهة لديها حادث متوسط الشدة.	جهتين أو أكثر لديها حادث مرتفع الشدة. **أو** أكثر من 5 جهات لديها حادث متوسط الشدة. **أو** إجمالي الأثر المالي للاحتيال أو سرقة الممتلكات يفوق 7 مليار جنيه سوداني.

ملحق رقم (4): الإخطار الأولي

الإخطار الأولي		
إسم الجهة		
إسم ومعلومات إتصال الشخص المسؤول عن الإستجابة للأزمات	الإسم	
	رقم الهاتف	
	البريد الإلكتروني	
تاريخ ووقت إرسال الإخطار	**التاريخ:** يوم/شهر/سنة	**الوقت:** ثانية:دقيقة:ساعة م/ص
الرقم المرجعي للحادث لدى الجهة (إن وجد)		
تصنيف شدة تأثير الحادث على الجهة	متوسط الشدة ☐	مرتفع الشدة ☐
وصف المشكلة: (بما في ذلك فئة الحادث (مثل: هجوم حجب الخدمة DDoS، التشويه، خرق المعلومات، وغيرها)، طريقة الهجوم، ومستوى انقطاع الخدمة، وإمكانية التحقيق أو العقوبة التنظيمية، الأثر على السمعة، والنسبة التقديرية للعملاء المتأثرين)		
الجدول الزمني للحوادث وطريقة اكتشافها		
وصف جهود التخفيف		
الوقت المقدر للحل		
المخاطر التي قد تُعيق الحل		
طلب مساعدة بنك السودان المركزي		

ملحق رقم (5): تقرير الحالة

تقرير الحالة		
إسم الجهة		
إسم ومعلومات إتصال الشخص المسؤول عن الإستجابة للأزمات	الإسم	
	رقم الهاتف	
	البريد الإلكتروني	
الوضع الحالي اعتباراً من (التاريخ والوقت)	**التاريخ:** يوم/شهر/سنة	**الوقت:** ثانية:دقيقة:ساعة م/ص
الرقم المرجعي للحادث لدى الجهة (إن وجد)		
تصنيف شدة تأثير الحادث على الجهة	متوسط الشدة ☐	مرتفع الشدة ☐
1. ما الذي حدث منذ آخر إخطار؟		
2. متى حدثت التغييرات؟		
3. أين حدثت التغييرات؟		
4. كيف، متى، ومن قام باكتشاف أي شئ جديد؟		
السبب		
1. ماهو فهمك الحالي حول سبب الحادث؟		
2. هل كان المصدر داخلياً، خارجياً، أم غير معروف؟		

تحديثات الأثر	
1. العمليات	
2. العملاء	
3. الموظفون	
4. البيانات/الأنظمة	
5. متطلبات الإخطار/الإتصال	
6. النواحي القانونية/التنظيمية	
7. السمعة	
تحديثات الإستجابة	
1. ماهي إجراءات الإستجابة المتخذة حتى الآن؟	
2. ما مدى فعالية محاولات التخفيف؟	

3. ماهي التحديات التي لا تزال قائمة لحل هذا الوضع؟	
4. ماهو الوقت المقدر حالياً لحل الوضع؟	
مستوى الشدة وإمكانية التصعيد	
1. كيف يمكن أن يزداد الوضع سوءاً؟	
2. ماهي الجهات و/أو الأنظمة الأخرى التي قد تتأثر؟	
أسئلة	
1. ماهي المعلومات الأخرى التي ينبغي لبنك السودان المركزي معرفتها؟	
2. ماهو الدعم الذي تحتاجه من بنك السودان المركزي؟	

ملحق رقم (6): تقرير التعافي

تقرير التعافي			
إسم الجهة			
إسم ومعلومات إتصال الشخص المسؤول عن الإستجابة للأزمات	الإسم		
	رقم الهاتف		
	البريد الإلكتروني		
الوضع الحالي اعتباراً من (التاريخ والوقت)	**التاريخ:** يوم/شهر/سنة	**الوقت:** ثانية:دقيقة:ساعة م/ص	
الرقم المرجعي للحادث لدى الجهة إن وجد			
تصنيف شدة تأثير الحادث على الجهة	متوسط الشدة ☐	مرتفع الشدة ☐	
1. وصف وتاريخ بدء الإستجابة للحادث والتعافي منه			
2. وصف خطة الإستجابة والإجراءات المتخذة			
3. الأطراف المشاركة في إجراءات الإستجابة			
4. الدور الذي قام به بنك السودان المركزي (إن وجد)			
5. الدور الذي قامت به أطراف ثالثة (إن وجد)			
6. نوع الحل (وصف نوع الحل)	مؤقت ☐ (وصف نوع الحل)	دائم ☐ (وصف نوع الحل)	

7. **الوقت المقدر الأصـــلي للحل** (كما هو موثق في الإخطار الأولي)	
8. **الوقت الفعلي للحل**	
9. **الأثر على قاعدة العملاء**	
10. **الأثر المالي**	
11. **الأثر على السمعة**	
12. **التحديات الملحوظة في عملية التعافي**	
13. **التدخلات القانونية/التنظيمية**	
14. **الدروس المســتفادة والإجراءات التنموية المخطط لها**	

ملحق رقم (7): نموذج تقرير الحوادث منخفضة الشدة

تقرير الحوادث منخفضة الشدة					
إسم الجهة					
إسم ومعلومات إتصال الشخص المسؤول عن الإستجابة للأزمات	الإسم				
	رقم الهاتف				
	البريد الإلكتروني				
الفترة الزمنية المشمولة	من يوم/شهر/سنة حتى يوم/شهر/سنة				
الحوادث	ملخص موجز عن الحادث	ملخص موجز عن إجراءات الإستجابة المتخذة للحادث	ملخص موجز عن آثار الحادث	ملخص الدروس المستفادة والإجراءات الإضافية المطلوبة نتيجة للحادث	
1. إكتشافات الفيروسات (Virus Discoveries)					
2. محاولات التصيد الإلكتروني (Fishing Attempts)					
3. مسح المنافذ (Port Scans)					
4. هجمات حجب الخدمة (Distributed Denial of Services "DDoS" Attacks)					
5. محاولات استخدام برمجيات التشفير (Cryptoware Attempts)					

6. محاولات استخدام برمجيات الفدية (Ransomware Attempts)				
7. محاولات استخدام البرمجيات الخبيثة (Malware Attempts)				
8. اكتشاف الخروقات (Breach Discoveries)				
9. أخرى (Other)				