Republic Of Iraq
CENTRAL BANK OF IRAQ

جمهورية العراق
البنك المركزي العراقي

البنك المركزي العراقي

دائرة تقنية المعلومات والمدفوعات
قسم السياسات والتنظيم والدراسات

NO : العدد : ٩٢٠٠/١٤
DATE : التاريخ : ٢٠٢٤/٦/١١

المصارف كافة

شركات مزوّدي خدمات الدفع الإلكتروني كافة

م/ ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق

Cyber Resilience Controls for the Financial and Banking Sector in Iraq

تحية طيبة..

انطلاقًا من الدور الرئيس للبنك المركزي العراقي في تنظيم القطاع المالي والمصرفي وتنميته وتطويره بمختلف نشاطاته الرقمية وعملياته التقنية والمعلوماتية، وسعيه المستمر لتعزيز الأمن السيبراني وحماية البيانات والمعلومات المتعلقة بالنظم المالية والمصرفية، ولوضع إطار عمل معياري وضوابط لتطوير قدرات الصمود السيبراني ومستويات الاستعداد لمواجهة التأثيرات الناتجة عن المخاطر والتهديدات والهجمات السيبرانية، والتصدي لها بفاعلية، وتعزيز مرونة المؤسسات المالية والمصرفية في التكيّف مع الاضطرابات التقنية والأمنية المعلوماتية السيبرانية وتحمّل هذه الأزمات والتعافي منها بمدد قياسية مناسبة، وضمان استمرارية مزاولة الأعمال والعمليات والنشاطات المصرفية.

وفي سبيل توفير إطار شامل لتنظيم هذا القطاع وتنميته وتطويره بما يتلاءم والتحديات التقنية الحديثة والتهديدات السيبرانية المتزايدة، نرفق ربطًا وثيقة ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق الواجب الالتزام بها لأجل تعزيز الصمود السيبراني لمؤسساتكم.

وتُعدُّ الضوابط والإرشادات والإجراءات والتدابير الواردة في هذه الوثيقة مرجعًا مهمًّا وأساسًا لحماية البنى التحتية التقنية والأنظمة المالية والمصرفية، وتسهم في تعزيز جاهزية مؤسساتكم ومرونتها في مواجهة التحديات التقنية

CBI Head Office : Al-Rasheed St. Baghdad - Iraq
Tel:8165171 Telephone Exchange With 4 Line
P.O Box: 64 Fax : 0096418166802
E-Mail : cbi@cbi.iq

مركز البنك : شارع الرشيد - بغداد - العراق
هاتف : ٨١٦٥١٧١ (بدالة مركزية ذات اربعة خطوط)
ص.ب : ٦٤ فاكس ٠٠٩٦٤١٨١٦٦٨٠٢
البريد الالكتروني: cbi@cbi.iq

والتهديدات الأمنية والسيبرانية والتكيُّف معها، والتنبؤ بمخاطرها، واحتوائها، والتعافي منها بسرعة، وضمان القدرة على مواصلة أداء المهام والوظائف وتقديم الخدمات بشكل مستمر.

.. مع التقدير.

المرفقات:

- ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق باللغتين العربية والانجليزية.

أ.د. عمار حمد خلف

نائب المحافظ وكالة

٢٠٢٤/٦/١١

CBI Head Office : Al-Rasheed St. Baghdad - Iraq
Tel:8165171 Telephone Exchange With 4 Line
P.O Box: 64 Fax : 0096418166802
E-Mail : cbi@cbi.iq

مركز البنك : شارع الرشيد - بغداد - العراق
هاتف : ٨١٦٥١٧١ (بدالة مركزية ذات اربعة خطوط)
ص.ب : ٦٤ فاكس ٠٠٩٦٤١٨١٦٦٨٠٢
البريد الالكتروني :cbi@cbi.iq

البنك المركزي العراقي
دائرة تقنية المعلومات والمدفوعات
قسم السياسات والتنظيم والدراسات

ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق

الطبعة الاولى
حزيران ٢٠٢٤

قائمة المحتويات

المصطلحات والتعاريف

المصطلح	التعريف
AML	Anti Money Laundering مكافحة غسل الاموال
BCP	Business Continuity Plan خطة استمرارية الاعمال
BIA	Business Impact Analysis تحليل تأثير الاعمال
BRD	Business Requirement Document وثيقة متطلبات الاعمال
CIO	Chief Information Officer المدير التنفيذي للمعلومات
CISO	Chief Information Security Officer كبير موظفي أمن المعلومات
CTO	Chief Technology Officer الرئيس التنفيذي للتكنولوجيا
DBA	Data Base Administrator مسؤول قاعدة البيانات
DBMS	Database Management System نظام ادارة قواعد البيانات
DC	Data Center مركز البيانات
DRP	Disaster Recovery Plan خطة التعافي من الكوارث
DRS	Disaster Recovery Site موقع التعافي من الكوارث
EMV	Europay, MasterCard and Visa, technical standard
HTTPS	Hypertext Transfer Protocol Secure بروتوكول النقل الآمن للنصوص الترابطية
IS	Information Systems أنظمة المعلومات
IT	Information Technology تقنية المعلومات
KPI	Key Performance Indicators مؤشرات الاداء الرئيسي
KRI	Key Risk Indicator مؤشر المخاطر الرئيسي
MFA	Multifactor Authentication المصادقة متعددة العوامل
NBFI	Non-Banking Financial Institution المؤسسات المالية غير المصرفية
OS	Operating System نظام التشغيل
OWASP	Open Worldwide Application Security Project مشروع أمان تطبيق الويب المفتوح

PCI DSS	PCI-DSS Payment Card Industry Data Security Standard معيار أمان بيانات صناعة بطاقات الدفع
RPO	Recovery Point Objective هدف نقطة الاسترجاع
RTGS	Real Time Gross Settlement نظام التسوية اللحظية
RTO	Recovery Time Objective هدف وقت الاسترجاع
SFTP	Secure File Transfer Protocol بروتوكول النقل الآمن للملفات
SSH	Secure Shell or Secure Socket Shell بروتوكول النقل الآمن
TLS	Transport Layer Security بروتوكول أمان طبقة النقل
UAT	User Acceptance Test اختبار قبول المستخدم
UVT	User Verification Test اختبار التحقق للمستخدم
VA	Vulnerability Assessment تقييم الضعف
VM	Virtual Machine الآلة الافتراضية
VPN	Virtual Private Network الشبكة الافتراضية الاحتياطية
WAF	Web Application Firewall جدار حماية تطبيقات الويب

المقدمة

الغرض من هذه الوثيقة هو التوجيه للمؤسسات والكيانات في القطاع المالي والمصرفي لتعزيز صمودها السيبراني. تهدف هذه الوثيقة أيضًا إلى توفير تفاصيل إضافية تتعلق بالتدابير التي يجب على مؤسساتكم اتخاذها لتعزيز قدرات الصمود السيبراني، بهدف التقليل من المخاطر المتصاعدة التي تشكلها التهديدات والهجمات السيبرانية على الاستقرار المالي والمصرفي، حيث يُسهم الصمود السيبراني في التنبؤ بالهجمات السيبرانية ومقاومتها واحتوائها والتعافي منها بسرعة. لتعزيز استقرار القطاع المالي والمصرفي والنمو الاقتصادي، من المهم التركيز على تقليل وتجنب المخاطر. إذا لم يتم إدارة المخاطر السيبرانية بشكل صحيح، فإن لديها القدرة على أن تصبح مصدرًا للاضطرابات المصرفية أو يمكن أن تصبح قناة رئيسية تنتقل من خلالها هذه الاضطرابات إلى الأسواق المالية المحلية والدولية. في هذا السياق، يعتبر مستوى إدارة الصمود السيبراني عاملاً حاسمًا في صمود النظام المالي والاقتصادي الشامل والعمل على نطاق أوسع لتقليل المخاطر وتعزيز الشفافية والاستقرار المالي.

من المهم تنمية ثقافة الصمود السيبراني في المؤسسات المالية والمصرفية، الصمود السيبراني هو قدرة المؤسسات على مواصلة أداء مهامها ووظائفها من خلال:

١. التنبؤ والتكيف مع المخاطر والتهديدات والهجمات السيبرانية أثناء حدوثها والتغييرات المرتبطة بالبيئة التقنية للمعلومات.
٢. الصمود والتحديد والكشف والاحتواء والاستجابة والتعافي السريع من الأحداث السيبرانية .

هذه الإرشادات مرجع مهم لمجلس الإدارة والإدارة العليا، لدورهم الفعال في ضمان الصمود السيبراني، وهذا الدليل أيضًا مرجع لجميع الموظفين المسؤولين عن تصميم ومراقبة وتنفيذ عناصر إطار عمل الصمود السيبراني.

مبادئ تنفيذ الأمن السيبراني الفعّال (Principles for effective cybersecurity (implementation

يجب اتباع المبادئ التالية لتنفيذ الإرشادات بشكل فعّال لأمن جميع الخدمات الحيوية والبنى التحتية الداعمة لها.

١. اعتبارات اصحاب المصلحة (Stakeholder Considerations)

على الرغم من أن هذا الدليل موجه مباشرة إلى المؤسسات والكيانات في القطاعين المالي والمصرفي، إلا أنه من المهم أيضًا أن تعزز هذه المؤسسات فهم أهداف الصمود السيبراني لدى المشاركين ومزودي الخدمات والمنتجات واصحاب المصلحة الآخرين، وأن تتخذ الإجراءات المناسبة لدعم التنفيذ، ان تحقيق حلول فعّالة يتطلب من المؤسسات أن تتعاون مع اصحاب المصلحة المعنيين المرتبطين بها لتعزيز إطارات عمل الصمود السيبراني.

نظرًا لأهمية الصمود السيبراني في دعم أهداف استقرار القطاع المالي والمصرفي، يجب على جميع المؤسسات ضمن القطاعين المالي والمصرفي تعزيز مفهوم التعاون مع اصحاب المصلحة على جميع المستويات وتبنّيه كنهج يساعد في تطوير الاستراتيجيات، والاستجابة بطريقة ملائمة وفعالة، وتنسيق الجهود، وتقديم التوجيه

والإشراف والعمل المشترك ضمن مجالات وإطار عمل الصمود السيبراني، ويُؤخذ في الاعتبار ناتج التعاون في الخطط الاستراتيجية في هذا الصدد.

٢. استدامة وتعزيز الصمود السيبراني (Sustaining and Enhancing Cyber Resilience)

يجب على المؤسسات اتخاذ تدابير مناسبة وسريعة ومستدامة لتعزيز الصمود السيبراني داخليًا وخارجيًا، سواء داخل المؤسسة (الأنظمة التقنية والمعلوماتية الداخلية والبنى التحتية)، أو مع المؤسسات والكيانات المرتبطة بها داخل القطاع، حيث تؤدي الترابطات الواسعة بين المؤسسات والكيانات في القطاعين المالي والمصرفي إلى نقل المخاطر بشكل عام وأمن المعلومات والأمن السيبراني بشكل خاص بينها، مع الحاجة إلى الاخذ بنظر الاعتبار العمليات المختلفة لتطوير الأمن التقني والمعلوماتي ومستويات الصمود السيبراني المختلفة بين هذه المؤسسات.

٣. الجهود المستمرة لتحسين الصمود السيبراني (Ongoing Efforts to Improve Cyber Resilience)

يجب على المؤسسات أن تتكيف وتطوّر وتحسّن وتعزز بشكل مستمر خطط وإطارات عمل الصمود السيبراني، لزيادة مستوى الحماية السيبرانية والمعلوماتية، ومنع الهجمات والتهديدات والانتهاكات واستغلال الثغرات ونقاط الضعف، وتحسين قدراتها على اكتشاف والاستجابة والاحتواء والتعافي من الهجمات السيبرانية والهجمات الإلكترونية الناجحة.

٤. النهج القائم على المخاطر (Risk-Based Approach)

قد تتأثر مكونات البنية التحتية للمعلومات والأنظمة والتطبيقات والأصول التقنية الأخرى بمستويات وأنواع مختلفة من المخاطر الإلكترونية والسيبرانية، حيث تختلف المخاطر ومستوياتها حسب الأجهزة والتقنيات والبرمجيات المستخدمة، ومزودي الخدمات، والمؤسسات، والكيانات المرتبطة، والمشاركين، والكوادر العاملة، ولذلك يجب على المؤسسات اعتماد نهج قائم على المخاطر وتحديد الأولويات للجهود والتدابير للتخفيف من المخاطر وتقليلها لتناسب المستويات المختلفة من المخاطر الإلكترونية والسيبرانية، مع الاخذ بنظر الاعتبار تنفيذ الإرشادات والتوجيهات في سياق الأطر القانونية والتنظيمية ذات الصلة بالإضافة إلى التعليمات والقوانين واللوائح المعتمدة والسارية المفعول.

مع الاخذ في الاعتبار مبادئ التصميم، تعتمد الإرشادات بشكل عام على إطار عمل الأمن السيبراني (NIST) ، حيث يمكن تجميع الأنشطة في فئات مثل التحديد، والحماية، والكشف، والاستجابة، والتعافي.

الحوكمة (Governance)

حوكمة تقنية المعلومات (IT Governance)

تعتبر الأدوار والمسؤوليات المحددة بوضوح لمجلس الإدارة والإدارة العليا أمرًا حاسمًا أثناء تنفيذ حوكمة تقنية المعلومات، حيث تمكن الأدوار المحددة بوضوح من التحكم الفعّال في المشاريع وتوقعات المؤسسات. تتضمن اصحاب المصلحة المعنيين بحوكمة تقنية المعلومات مجلس الإدارة (Board of Directors)، الرئيس التنفيذي

(CEO)، لجنة الإرشاد لتقنية المعلومات (IT Steering Committee)، لجنة الأمن السيبراني (Cybersecurity Committee)، المدير التنفيذي للمعلومات (CIO)، مدير تقنية المعلومات (CTO)، مدير أمن المعلومات والأمن السيبراني (CISO)، لجنة إدارة المخاطر (Risk Management Committee)، مسؤول إدارة المخاطر(Chief Risk Officer)، والمسؤولين التنفيذيي (Business Executives).

أدوار ومسؤوليات مجلس الإدارة (Roles and Responsibilities of Boards of Directors)

أ) الموافقة على وثائق استراتيجيات وسياسات تقنية المعلومات.

ب) التأكد من أن الإدارة قد وضعت عملية تخطيط فعالة.

ج) تأييد أن استراتيجية تقنية المعلومات متوافقة فعلاً مع استراتيجية الأعمال.

د) التأكد من أن هيكلية تنظيم تقنية المعلومات وتكمّل وتتوافق مع نموذج الأعمال واتجاهها.

ه) التأكد من أن استثمارات تقنية المعلومات تمثل توازنًا بين المخاطر والفوائد والميزانيات المقبولة.

و) التأكد من حالة الامتثال لسياسة الأمن السيبراني.

أدوار ومسؤوليات لجنة الإرشاد لتقنية المعلومات (Roles and Responsibilities of IT Steering Committee)

يجب تشكيل لجنة الإرشاد لتقنية المعلومات بمشاركة ممثلين من اقسام تقنية المعلومات، وإدارة المخاطر، والموارد البشرية، والتدقيق الداخلي، والقسم القانوني، والاقسام الأخرى ذات الصلة.

أ) مراقبة منهجيات الإدارة لتحديد وتحقيق الأهداف الاستراتيجية.

ب) يكونون على دراية بالتعرض لمخاطر تقنية المعلومات والضوابط الخاصة بها .

ج) تقديم التوجيهات المتعلقة بالمخاطر والتمويل ومصادره.

د) التأكد من أولويات المشاريع وتقييم الجدوى لمقترحات تقنية المعلومات .

ه) التأكد من أن جميع المشاريع الحيوية تحتوي على عنصر لـ "إدارة مخاطر المشروع " (Project Risk Management).

و) استشارة وتقديم المشورة بشأن اختيار التقنيات ضمن المعايير .

ز) التأكد من اتمام تقييمات نقاط الضعف والثغرات للتقنيات الجديدة.

ح) ضمان الامتثال للمتطلبات التنظيمية والقانونية.

ط) اعطاء التوجيهات والتأكد من ان تصميم بنية ومعمارية تقنية المعلومات تمتثل وتتوافق مع متطلبات الامتثال التشريعي والتنظيمي (legislative and regulatory compliance requirements).

حوكمة أمن المعلومات (Information Security Governance)

يجب تشكيل لجنة الأمن السيبراني بمشاركة ممثلين من اقسام تقنية المعلومات (IT)، وأمن المعلومات والأمن السيبراني (information and cybersecurity)، وإدارة المخاطر (Risk management)، ولجنة الشكاوى الداخلية (Internal complaints committee- ICC)، والاقسام الاخرى ذات الصلة.

أدوار ومسؤوليات لجنة الأمن السيبراني (Roles and Responsibilities of Cybersecurity (Committee

أ) ضمان تطوير وتنفيذ أهداف الأمن السيبراني، وسياسات وإجراءات الأمن السيبراني ذات الصلة.

ب) تقديم الدعم الإداري المستمر لعمليات أمن المعلومات.

ج) ضمان الامتثال المستمر لأهداف الأعمال، والمتطلبات التنظيمية والقانونية ذات الصلة بالأمن السيبراني.

د) دعم صياغة إطار/عملية إدارة مخاطر تقنية المعلومات (IT risk management framework/process) وتحديد عتبات الخطر المقبولة (Risk Apatite).

ه) المراجعة الدورية واعطاء الموافقة على تعديلات عمليات الأمن السيبراني.

سياسات ومعايير وإجراءات تقنية المعلومات (IT Policy, Standard and Procedure)

أ) يجب على كل مؤسسة أن يكون لديها "سياسة الأمن السيبراني" متوافقة مع توجيهات الأمن السيبراني وموافق عليها من قبل مجلس الإدارة.

ب) تغطي هذه السياسة التقنيات الشائعة مثل الحواسيب والاجهزة الطرفية، والبيانات والشبكة، والتطبيقات، وغيرها من الموارد التقنية المتخصصة، يعتمد تقديم خدمات المؤسسات على توافرية وموثوقية وسلامة نظام المعلومات الخاص بها. لذلك، يجب على كل مؤسسة اعتماد الضوابط المناسبة لحماية نظام المعلومات الخاص بها. يجب على الإدارة العليا للمؤسسة التعبير عن التزامها بالأمن السيبراني من خلال ضمان برنامج مستمر للتوعية والتدريب لكل مستوى من مستويات الموظفين والأطراف المعنية .

ج) تتطلب السياسة تحديثات منتظمة للتعامل مع التغيرات المتطورة في بيئة تقنية المعلومات داخل المؤسسة بشكل خاص وعلى مستوى القطاع المالي والمصرفي بشكل عام.

د) يجب على المؤسسة توظيف متخصصين في الأمن السيبراني في قسم أمن المعلومات للتعامل بشكل احترافي ونزيه مع الاحداث الامنية، وتوثيق السياسات، والمخاطر التقنية الأساسية، ومعالجة المخاطر، وغيرها من الأنشطة ذات الصلة.

ه) بالنسبة لقضايا عدم الامتثال، يجب تقديم خطة الامتثال إلى البنك المركزي العراقي لطلب الاستثناء، ويجب أن يكون الاستثناء لفترة محددة.

التوثيق (Documentation)

أ) يجب أن يكون للمؤسسة المالية هيكل تنظيمي محدّث لقسم تقنية المعلومات.

ب) يجب أن يكون للمؤسسة المالية وحدة دعم تقنية المعلومات في الهيكل التنظيمي لفروعها.

ج) يجب أن يكون لكل من يعمل في قسم تقنية المعلومات وصف وظيفي مع موظف بديل.

د) يجب على المؤسسة المالية الحفاظ على عزل الواجبات لمهام تقنية المعلومات.

ه) يجب على المؤسسة المالية الحفاظ على وثائق تصميم مفصّلة لجميع الأنظمة/الخدمات التقنية الحيوية (على سبيل المثال، تصميم مركز البيانات، تصميم الشبكة، مخطط الطاقة لمركز البيانات، إلخ.).

و) يجب على المؤسسة المالية أن يكون لديها جدول زمني مسبق للمهام التقنية الحسّاسة (على سبيل المثال، عمليات نهاية اليوم (EOD)، مراقبة الشبكة (Network monitoring)، الأمن المادي لمركز البيانات (Physical security for Data Center)، مراقبة أجهزة الصراف الآلي (ATM monitoring)، إلخ.).

ز) يجب على المؤسسة الحفاظ على "إجراءات التشغيل" المحدّثة لجميع الأنشطة الوظيفية لتقنية المعلومات (على سبيل المثال، إدارة النسخ الاحتياطي، إدارة قواعد البيانات، إدارة الشبكة، جدولة العمليات، بدء تشغيل النظام، إيقاف التشغيل، إعادة التشغيل، والتعافي).

ح) يجب أن يكون للمؤسسة استمارات طلبات/ اقرارات (requisition/acknowledgement forms) لمختلف الطلبات/العمليات/الخدمات التقنية.

ط) يجب أن يكون للمؤسسة دليل المستخدم لجميع التطبيقات للمستخدمين الداخليين/الخارجيين.

١. إدارة البنية التحتية لتقنية وأمن المعلومات (IT and Security Infrastructure Management)

يجب على إدارة الأمن السيبراني التأكد من أن وظائف وعمليات تقنية المعلومات تُدار بكفاءة وفعالية، يجب على المؤسسات أن تكون على علم بقدرات تقنية المعلومات وأن تكون قادرة على تقدير وفهم الفرص والمخاطر المحتملة للاستخدام السيئ. يجب عليهم ضمان الحفاظ على التوثيق الصحيح، بالخصوص للأنظمة التي تدعم المعاملات المالية والتقارير. يجب عليهم المساهمة في التخطيط للأمن السيبراني لضمان توزيع الموارد بما يتماشى مع أهداف الأعمال ولضمان توظيف موظفين تقنيين كفوئين بما يكفي بحيث لا يكون استمرار عمل تقنية المعلومات عرضة لمخاطر جسيمة بشكل مستمر. تتعامل إدارة الأمن السيبراني مع الأدوار والمسؤوليات، وسياسة الأمن السيبراني، والوثائق، والتدقيق الداخلي والخارجي لنُظم المعلومات، والتدريب والتوعية، والمخاطر التقنية.

يعد مجال تقنية المعلومات عرضة لأشكال مختلفة من الهجمات. يجب على المؤسسة تنفيذ حلول أمنية على مستوى البيانات، والتطبيقات، وقواعد البيانات، وأنظمة التشغيل، والشبكات لمعالجة التهديدات ذات الصلة بشكل كافٍ. يجب تنفيذ تدابير مناسبة لحماية المعلومات الحساسة أو السرية مثل بيانات الزبائن الشخصية، وبيانات الحسابات والمعاملات التي يتم تخزينها ومعالجتها في الأنظمة. يجب التحقق من هوية الزبائن بشكل صحيح قبل الوصول إلى المعاملات عبر الإنترنت، أو المعلومات الشخصية الحساسة أو المعلومات الخاصة بالحسابات. يجب على المؤسسة أن يكون لديها آلية لقياس أداء حوكمة الأمن السيبراني والضوابط التقنية عن طريق قياس مؤشرات الأداء الرئيسية (Key Performance Indicators-KPI’s) التالية على الأقل.

١. عدد اجتماعات لجنة الحوكمة المخطط لها مقابل التي تم إجراؤها.

٢. النسبة المئوية الفقرات المنجزة الناتجة عن اجتماعات لجنة الحوكمة .

٣. حالة التقدم في مشاريع/مبادرات أمن المعلومات (نسبة الإنجاز).

٤. اجمالي النسبة المئوية للموظفين الذين وافقوا على سياسة قبول المستخدم في الربع الأخير.

٥. النسبة المئوية من سياسة أو إجراءات أمن المعلومات التي تمت مراجعتها/الموافقة عليها في الوقت المحدد.

٦. عدد الاستثناءات من تطبيق السياسات التي تم اغلاقها او مراجعتها.

٧. النسبة المئوية للحوادث التي تم تحديدها خلال الشهر الماضي والتي تتعلق بعدم الالتزام بأي من سياسات وإجراءات أمن المعلومات الحالية.

٨. نسبة اعضاء الإدارة العليا (Top management)/ أصحاب الأعمال (Business owners) المشاركين في برنامج أمن المعلومات.

٩. النسبة المئوية مشاريع الأمن السيبراني التي تم مراجعتها وتقييمها خلال الربع الأخير.

١٠. النسبة المئوية تقييم مخاطر مشاريع الأمن السيبراني المكتملة في الربع الأخير.

١١. نسبة المئوية للحوادث التي نتجت عن نقص الموارد المؤهلة لأمن المعلومات.

١٢. التوجيه المتخذ في عدد الموظفين الذين لم يشاركوا بنجاح في البرنامج التوعوي والتدريبي.

١٣. النسبة المئوية الحملات التوعوية بأمن المعلومات التي تم تنفيذها بنجاح.

١٤. النسبة المئوية لتدريبات أمن المعلومات المخطط لها مقابل الفعلية.

١٥. النسبة المئوية لمتطلبات التدريب على أمن المعلومات التي تم تحقيقها بنتائج مرضية.

١٦. النسبة المئوية للمخاطر التي ظهرت في تقييم المخاطر السابق والحالي والتي تغيرت إلى مستوى أقل

١٧. النسبة المئوية المخاطر التي ظهرت في تقييم المخاطر السابق والحالي والتي تغيرت إلى مستوى أعلى.

١٨. التوجيه المتخذ في عدد الحالات التي لم يتم فيها إجراء تقييم المخاطر أو مراجعتها أو تحديثها كما هو مخطط له.

١٩. النسبة المئوية للمخاطر الجديدة التي تم تحديدها عند مراجعة أو تحديث تقييم المخاطر فيما يتعلق بجميع المخاطر التي كان ينبغي تحديدها من قبل وتم التغاضي عنها أو التي تم تقييمها بشكل غير صحيح.

٢٠. النسبة المئوية لجميع السجلات (تقارير التدقيق، تقارير الحوادث، السجلات، الأحداث، إلخ) التي تشير إلى أن أيّ من الضوابط التي تم تحديدها على أنها "غير قابلة للتطبيق" ستكون مطلوبة حالياً.

٢١. النسبة المئوية لجميع الحالات خلال العام الماضي التي لم يتم فيها تحديث تقييم مخاطر أمن المعلومات و/أو معالجة المخاطر على الرغم من جدولتها وحدوث تغييرات كبيرة.

٢٢. النسبة المئوية للعمليات والاعمال التي بدأ تقييم المخاطر لها في الربع الأخير.

٢٣. عدد حالات قبول المخاطر التي تم إغلاقها/مراجعتها في الوقت المحدد

٢٤. النسبة المئوية لمعالجة المخاطر التي تم تنفيذها مقارنة بالمخطط لها في الربع الأخير.

٢٥. النسبة المئوية من قبول المخاطر التي تم إغلاقها مقابل المخطط لها في الربع الأخير

٢٦. مدى نشر سياسة الامتثال والتقييم واعتمادها في المؤسسة.

٢٧. مقدار الوقت والموارد التي قضاها القسم القانوني في إدارة قضايا الامتثال القانوني فيما يتعلق بأمن المعلومات.

٢٨. الانتهاء من التقييم الذاتي السنوي

٢٩. النسبة المئوية لحالات عدم الامتثال المبلغ عنها مقابل تلك التي تم معالجتها مقارنة بمعالجة نتائج التدقيق.

٣٠. النسبة المئوية لحالات عدم الامتثال المبلغ عنها مقابل تلك التي تم تخفيفها مقارنة بتقييمات الامتثال لأمن المعلومات.

٣١. النسبة المئوية ضوابط إدارة أمن المعلومات التي تم تنفيذها.

٣٢. النسبة المئوية لنتائج التدقيق المتكررة.

٣٣. النسبة المئوية الموظفين والمتعاقدين والأطراف الثالثة الذين قرأوا وقبلوا قواعد سلوك الموارد البشرية.

٣٤. النسبة المئوية لحسابات المستخدمين االموظفين والمتعاقدين والاطراف الثالثة التي تم حظرها بعد الإنتهاء.

٣٥. النسبة المئوية لحسابات الموظفين والمتعاقدين والمستخدمين الخارجيين الذين تم تعديل ملفاتهم الشخصية بناءً على تغيير ادوارهم.

٣٦. النسبة المئوية لاجراءات المراجعة والتحقق ماقبل التوظيف التي تم إجراؤها مقابل عدد الموظفين الجدد المعينين في الربع الأخير.

٣٧. النسبة المئوية من الأجهزة المحمولة التي تم منحها حق الوصول إلى الشبكة والانظمة والتطبيقات ونسبة مراجعتها وفقًا لسياسة استخدام الاجهزة الشخصية (BYOD) في العام الماضي.

٣٨. النسبة المئوية لمعدات الحوسبة المحمولة (مثل الهواتف الذكية وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية) التي تتوافق تمامًا مع المتطلبات ذات الصلة في سياسة التحكم في الوصول.

٣٩. النسبة المئوية من وسائط التخزين التي تم التخلص منها باستخدام تقنيات عدم الاسترجاع (المسح الآمن، التدمير) في الربع الأخير.

٤٠. عدد خدمات التجارة الإلكترونية الخاضعة لسياسة ادارة الاحداث لأمن المعلومات.

٤١. تقرير عن فترات تشغيل الخدمات المصرفية عبر الانترنت.

٤٢. النسبة المئوية للحوادث داخل المؤسسة حيث تتوفر معلومات كافية ودقيقة في نظام ادارة المعلومات و الاحداث الامنية (SIEM) لاكتشاف الحادث وإدارته.

٤٣. النسبة المئوية لحوادث أمن المعلومات التي تم الإبلاغ عنها خلال الإطار الزمني المطلوب وحسب فئات الحوادث مطبق على النحو المحدد في سياسة إدارة حوادث أمن المعلومات.

٤٤. النسبة المئوية للأحداث المشبوهة والشاذة التي تم تحديدها في الأنظمة والتطبيقات وقواعد البيانات المهمة.

٤٥. النسبة المئوية للأنظمة والتطبيقات وقواعد البيانات التي تم فيها تمكين/دمج الأحداث الأمنية في نظام ادارة المعلومات و الاحداث الامنية (SIEM).

٤٦. تكرار حالات الفشل التشغيلي التي تؤدي إلى حوادث أمن المعلومات.

٤٧. النسبة المئوية للحوادث التي تم حلها في الوقت المناسب (وفقًا لأوقات الاستجابة/الحل المحددة) حسب خطورة الحادث في الربع الأخير.

٤٨. النسبة المئوية للحوادث التي تم تحديد الأسباب الجذرية لها واكمالها.

٤٩. النسبة المئوية للتهديدات الناشئة في مجال استخبارات التهديدات (مؤشرات الاختراق-IOC's) التي تم تحديدها مقابل التي تم علاجها.

٥٠. النسبة المئوية للتهديدات الناشئة في مجال استخبارات التهديدات التي تم تصحيحها ومعالجتها.

٥١. النسبة المئوية لنقاط الضعف التي تم تحديدها ومعالجتها خلال الفترات الزمنية المقبولة كما هو محدد في المتطلبات الأمنية.

٥٢. النسبة المئوية لأنظمة مركز البيانات التي تم التخطيط لتغطيتها في تقييم نقاط الضعف.

٥٣. النسبة المئوية من أنظمة الاجهزة الطرفية التي تم التخطيط لتغطيتها في تقييم نقاط الضعف.

٥٤. النسبة المئوية لأنظمة مركز البيانات (DC) المخطط تغطيتها لتقييم نقاط الضعف المصادق عليه.

٥٥. النسبة المئوية من محطات العمل (workstations) المخطط تغطيتها لتقييم نقاط الضعف المصادق عليه.

٥٦. النسبة المئوية لنتائج تقييم نقاط الضعف في مراكز البيانات التي تم تحديدها مقابل التي تم معالجتها.

٥٧. النسبة المئوية لنتائج تقييم نقاط الضعف في الاجهزة الطرفية التي تم تحديدها مقابل التي تم معالجتها.

٥٨. النسبة المئوية للاجهزة التي تم تحديد نتائج تقييم الثغرات الأمنية لمراكز البيانات المعتمدة فيها مقابل معالجتها.

٥٩. النسبة المئوية للأنظمة الخارجية المخطط شمولها باختبارات الاختراق.

٦٠. النسبة المئوية للأنظمة الحرجة الداخلية المخطط شمولها باختبارات الاختراق.

٦١. النسبة المئوية من نتائج اختبارات الاختراق للانظمة الخارجية التي تم تحديدها مقابل التي تم معالجتها.

٦٢. النسبة المئوية من نتائج اختبارات الاختراق للانظمة الداخلية التي تم تحديدها مقابل التي تم معالجتها.

٦٣. النسبة المئوية للحوادث الأمنية التي تم الإبلاغ عنها، والتحقيق فيها، وإغلاقها.

٦٤. نسبة تكرار خروقات أمن المعلومات المتعلقة بالأمن المادي والبيئي.

٦٥. النسبة المئوية للعمليات التي تم حلها/إغلاقها/ تصحيحها للمكونات المعرضة للخطر والتي تم تحديدها من خلال المسوحات الدورية لمواقع الأمن المادي.

٦٦. عدد الحوادث/نتائج التدقيق التي تم تحديدها للعمليات غير المصرح بها لأصول المعلومات أو غيرها من القضايا المتعلقة بأمن المعلومات.

٦٧. النسبة المئوية من أصول المعلومات التي تم تصنيفها وحمايتها بشكل كافٍ.

٦٨. مدى نشر واعتماد سياسة إدارة الأصول في المؤسسة.

٦٩. نسبة الموظفين الذين يسمح لهم بالوصول إلى أنظمة المعلومات بعد التوقيع على إقرار بأنهم قرأوا وفهموا قواعد السلوك.

٧٠. النسبة المئوية للوسائط المادية المخصصة للنسخ الاحتياطي/ الارشفة المشفرة بالكامل.

٧١. النسبة المئوية لأصول المعلومات المصنفة مع الملكية (Ownership) والوصاية / الحافظ (Custodianship) للأنظمة المضافة حديثًا مقابل إجمالي عدد الأصول الجديدة المضافة في البنية التحتية التقنية للمؤسسة.

٧٢. النسبة المئوية للأشخاص الذين لا يلتزمون بسياسة تصنيف المعلومات وتسمية فئاتها والتعامل معها.

٧٣. تكرار حوادث أمن المعلومات التي تحدث ضمن عمليات تبادل المعلومات والتي يتم فيها الكشف عن المعلومات عن قصد أو عن غير قصد.

٧٤. النسبة المئوية من مراجعة متطلبات التطبيقات التي تمت خلال ٦ أشهر.

٧٥. النسبة المئوية من مراجعات متطلبات البنية التحتية التي تم إجراؤها خلال ٦ أشهر.

٧٦. عدد المحاولات المحظورة للوصول غير المصرح به.

٧٧. مدى نشر واعتماد سياسة التحكم في الوصول في المؤسسة.

٧٨. عدد طلبات تغيير الوصول التي تم تنفيذها مقابل التي لم يتم تنفيذها.

٧٩. إحصائيات جدار الحماية مثل النسبة المئوية لحزم البيانات المنتقلة لخارج الشبكة أو الجلسات المحظورة (على سبيل المثال، محاولة الوصول إلى مواقع الويب المدرجة في القائمة السوداء؛ وعدد هجمات القرصنة المحتملة التي تم صدها).

٨٠. عدد المحاولات المحظورة للوصول غير المصرح به إلى أنظمة التشغيل والتطبيقات والمعلومات وغيرها.

٨١. عدد التغييرات الطارئة.

٨٢. عدد التغييرات غير الناجحة في بيئات الإنتاج الفعلية (الحية) مقابل إجمالي عدد التغييرات الموافق عليها.

٨٣. النسبة المئوية تنفيذ الأنظمة الفعّالة المقبولة في الخدمة مع تنفيذ كافة المتطلبات الأمنية.

٨٤. النسبة المئوية لأنظمة المعلومات المتوافقة مع سياسة شراء وتطوير وصيانة نظم المعلومات.

٨٥. النسبة المئوية للأنظمة التي تم تقييمها على أنها متوافقة تمامًا مع سياسة أمن التطبيقات.

٨٦. النسبة المئوية لإصدارات أنظمة التشغيل القديمة المستخدمة في البنية التحتية للمؤسسة.

٨٧. النسبة المئوية للنسخ الاحتياطي الناجح للبيانات.

٨٨. النسبة المئوية للانظمة المعلوماتية التي تحتوي على برامج مكافحة الفايروسات محدّثة.

٨٩. النسبة المئوية للأجهزة الشبكية التي تتوافق مع جميع متطلبات إدارة أمن الشبكة.

٩٠. النسبة المئوية للأنظمة التي تحتوي على بيانات قيّمة/حساسة والتي تم تنفيذ ضوابط التشفير المناسبة لها بشكل كامل.

٩١. النسبة المئوية لتقييمات مخاطر الاطراف الخارجية التي تم إجراؤها في العام الماضي.

٩٢. نسبة تكرار حوادث أمن المعلومات التي تتعلق بأطراف خارجية.

٩٣. النسبة المئوية لتوقيع اتفاقيات NDA مع البائعين والمتعاقدين والاطراف الخارجية.

٩٤. النسبة المئوية لاتفاقيات مستوى الخدمة التي تستوفي جميع متطلبات الأمن السحابي ذات الصلة.

٩٥. نسبة مقاييس الأداء الناجحة المطبقة.

٩٦. نسبة جميع حالات عدم المطابقة مع متطلبات أمن المعلومات التي تم اكتشافها ولم يتم حلها خلال الإطار الزمني المخطط لها.

٢. إدارة المخاطر (Risk Management)

يجب أن تمتلك المؤسسات والكيانات في القطاع المالي والمصرفي إطار عمل يوضح كيفية تعريف أهداف الصمود السيبراني واستيعاب واحتواء المخاطر السيبرانية، بالإضافة إلى كيفية تحديد المخاطر السيبرانية والتحقق من صحتها وإدارتها بشكل فعّال، ودعم اهداف الاستقرار المالي والمصرفي مع ضمان الكفاءة والفعالية والجدوى الاقتصادية لتحقيقها، يهدف إطار عمل الصمود السيبراني إلى الحفاظ على قدرة المؤسسات المصرفية وتعزيزها على التوقع للهجمات السيبرانية، ومقاومتها، واحتوائها، والتعافي منها، وتقليل احتمال حدوث أي تأثير لهجوم سيبراني ناجح على عملياتها وأنظمتها وتطبيقاتها من جهة، وعلى المؤسسات والكيانات المرتبطة بها من جهة أخرى، ويجب مراجعة إطار عمل الصمود السيبراني وتحديثه بشكل دوري لضمان أنه لا يزال مناسبًا وفعالًا، ويجب على مجلس الإدارة والإدارة العليا اعتماد هذا الإطار لضمان توافقه مع استراتيجية الصمود السيبراني.

مخاطر تقنية المعلومات هي احد مكونات مجموعة المخاطر الشاملة للمؤسسة. المخاطر الأخرى التي تواجهها المؤسسة المالية تشمل المخاطر الاستراتيجية والبيئية والسوقية والائتمانية والتشغيلية ومخاطر الامتثال، إلخ. المخاطر المتعلقة بتقنية المعلومات هي جزء من المخاطر التشغيلية. ومع ذلك، حتى المخاطر الاستراتيجية تحتوي على مخاطر تقنيات معلومات، خاصة عندما تكون تقنية المعلومات هي العامل الرئيسي والممكّن للمبادرات التجارية الجديدة. وتتألف من الأحداث والظروف المتعلقة بتقنية المعلومات التي قد تؤثر بشكل محتمل على الأعمال. يمكن أن تحدث بصورة متكررة وبحجم غير متوقع، وتخلق تحديات في تحقيق الأهداف الاستراتيجية.

٢,١. وظائف الأعمال والدعم (Business and Supporting Functions)

يجب على المؤسسات المالية تحديد مهام عملها والعمليات المساندة لها . تؤدي وظائف الأعمال أنشطة المؤسسات المالية التي تحقق دخلاً من خلال الخدمات المقدمة للزبائن. عادةً ما تشكل وظائف الأعمال الأساسية النشاط الأساسي للمؤسسة، لكن قد تتضمن أيضًا أنشطة أخرى (ثانوية) إذا اعتبرت المؤسسة هذه الأنشطة جزءًا من وظائفها الأساسية .

إجراء تقييم للمخاطر المرتبطة بها وتصنيف المهام والعمليات وفقًا لمستوياتها الحساسة والحرجة، والتي تمكّن المؤسسات من تحديد أولويات الحماية، والتحقيق، والاستكشاف، والاستجابة، وجهود التعافي من الكوارث.

٢,٢. المخاطر الناشئة عن الارتباطات (Risk from Interconnections)

تلتزم المؤسسات المالية والمصرفية بتنفيذ تدابير وقائية، وتدابير الحماية، وتخفيف وتقليل المخاطر الناشئة عن الكيانات المرتبطة بها وفقًا لنوع العمل وطريقة الارتباط، بما في ذلك العلاقة والترابط بين المؤسسة وكياناتها المرتبطة بها، لغرض تجنب المخاطر وتقليلها وتخفيفها بشكل عام والمخاطر السيبرانية بشكل خاص، يعتبر مستوى وضوابط وعمليات واجراءات الصمود السيبراني هو جزء لا يتجزأ من اتفاقيات المؤسسة (العقود، اتفاقيات مستوى الخدمة، اطارات العلاقة ومجال الارتباط، المخاطر) مع الكيانات المرتبطة بها، على سبيل المثال لا الحصر المؤسسات المالية والمصرفية الأخرى، والبائعين، ومقدمي الخدمات، وتخضع هذه الاتفاقيات لإجراءات التدقيق والتقييم الدورية للمخاطر السيبرانية وفقًا لإطار عمل الصمود السيبراني والمعايير الأمنية المعتمدة والضوابط.

٢,٣. إدارة أمن الموردين والأطراف الخارجية (Supplier and Third-Party Security (Management

يجب على المؤسسات المالية والمصرفية إجراء تقييم للمخاطر بشكل عام وأمن المعلومات والأمن السيبراني المتعلقة بالبائعين والموردين ومقدمي الخدمات والأطراف الخارجية الأخرى، وتطبيق وتنفيذ الضوابط لاكتشاف ومنع الاختراقات والهجمات السيبرانية المرتبطة بتلك الكيانات.

٢,٤. حوكمة مخاطر تقنية المعلومات (IT Risk Governance)

٢,٤,١ يجب ان تشكل المؤسسة لجنة إدارة مخاطر تقنية المعلومات لحوكمة كل مخاطر تقنية المعلومات وتدابير التخفيف والتقليل ذات الصلة.

٢,٤,٢ يجب على المؤسسة أن تحدد مدى تقبل المخاطر (مقدار المخاطر التي تكون المؤسسة مستعدة لقبولها لتحقيق أهدافها) من حيث تواتر وحجم المخاطر لاستيعاب الخسائر، مثل الخسارة المالية والضرر بالسمعة.

٢,٤,٣ يجب على المؤسسة تحديد درجة التسامح/تحمل المخاطر (الانحراف المسموح به عن المستوى المحدد لمدى تقبّل المخاطر) بعد موافقة مجلس الإدارة/لجنة إدارة المخاطر وإبلاغها بوضوح لجميع أصحاب المصلحة.

٢,٤,٤ يجب على المؤسسة مراجعة واعتماد التغير في مدى تقبل المخاطر والتسامح/ تحمل المخاطر مع مرور الوقت؛ خاصة بالنسبة للتقنيات الجديدة والهيكل التنظيمي الجديد واستراتيجية العمل الجديدة وغيرها من العوامل التي تتطلب من المؤسسة إعادة تقييم ملف المخاطر الخاص بها على فترات منتظمة .

٢,٤,٥ يجب على المؤسسة تحديد مسؤوليات المخاطر للأفراد لضمان اكمالها بنجاح .

٢,٤,٦ يجب على المؤسسة تحديد مسؤولية المخاطر التي تنطبق على أولئك الذين يمتلكون الموارد المطلوبة ولديهم تخويل للموافقة على تنفيذ و/أو قبول نتيجة نشاط ما ضمن عمليات مخاطر تقنية المعلومات المحددة. وتبقى ملكية المخاطر مع المالك أو الوصي الذي يكون في الموقع الأفضل للتخفيف والتقليل من المخاطر المحددة لاصول معينة لتقنية المعلومات.

٢,٤,٧ يجب أن تقرّ المؤسسة بجميع المخاطر عن طريق التوعية بالمخاطر بحيث تكون مفهومة ومعروفة جيدًا ومحددة كوسيلة لإدارتها .

٢,٤,٨ يجب أن تساهم المؤسسة في توضيح التعرض الفعلي لمخاطر تقنية المعلومات للإدارة التنفيذية من خلال التواصل المفتوح، مما يتيح تحديد الاستجابات المناسبة والحكيمة للمخاطر .

٢,٤,٩ يجب على المؤسسة أن تكون على دراية من بين جميع أصحاب المصلحة الداخليين بأهمية تكامل المخاطر والفرص في مهامهم اليومية .

٢,٤,١٠ يجب أن تتحلى المؤسسة بالشفافية أمام أصحاب المصلحة الخارجيين فيما يتعلق بالمستوى الفعلي للمخاطر والعمليات المستخدمة لإدارة المخاطر .
٢,٤,١١ يجب على المؤسسة أن تبدأ ثقافة الوعي بالمخاطر من الأعلى مع مجلس الإدارة والمديرين التنفيذيين الذين يحددون التوجهات ويعلنون عن اتخاذ القرارات الواعية بالمخاطر ويكافئون السلوكيات الفعّالة لإدارة المخاطر .
٢,٤,١٢ تقوم إدارة قسم أمن المعلومات بإبلاغ لجنة أمن تقنية المعلومات ولجنة إدارة المخاطر بحالة المخاطر الأمنية لتقنية المعلومات بشكل دوري على النحو المحدد في السياسة.

٢,٥. تقييم مخاطر تقنية المعلومات (IT Risk Assessment)

تتطلب تقييمات مخاطر تقنية المعلومات والقرارات القائمة على المخاطر الفعالة أن يتم التعبير عن مخاطر تقنيات المعلومات بطريقة واضحة وغير غامضة وبمصطلحات ذات صلة بالأعمال، وتتطلب الإدارة الفعالة للمخاطر تفاهماً متبادلاً بين تقنية المعلومات والأعمال حول المخاطر التي يجب إدارتها، يجب أن يكون لدى جميع أصحاب المصلحة القدرة على الفهم والتعبيرعن كيفية تأثير الأحداث الضارة على أهداف العمل .
أ) يجب أن تفهم فرق تقنية المعلومات كيف يمكن أن تؤثر الإخفاقات أو الأحداث المتعلقة بتقنية المعلومات على أهداف المؤسسة وتتسبب في خسارة مباشرة أو غير مباشرة للمؤسسة .
ب) يجب أن تفهم فرق الأعمال كيف يمكن أن تؤثر الإخفاقات أو الأحداث المتعلقة بتقنية المعلومات على الخدمات والعمليات الرئيسية .
٢,٥,١ يجب على المؤسسة إنشاء احتياجات تحليل الاثر على الاعمال (Business Impact Analysis) لفهم آثار الأحداث الضارة. يمكن للمؤسسة أن تمارس العديد من التقنيات والخيارات التي يمكن أن تساعدها على وصف مخاطر تقنية المعلومات باتجاهات الاعمال .
٢,٥,٢ يجب على المؤسسة ممارسة تطوير واستخدام تقنية سيناريوهات المخاطر لتحديد المخاطر المهمة وذات الصلة. يمكن انشاء واستخدام سيناريوهات المخاطر أثناء تحليل المخاطر حيث يتم تقييم تكرار وتأثير هذه السيناريوهات .
٢,٥,٣ يجب على المؤسسة تحديد عوامل المخاطر التي تؤثر على تكرار و/أو تأثير سيناريوهات المخاطر على الاعمال.
٢,٥,٤ يجب على المؤسسة أن تفسر عوامل المخاطر على أنها عوامل مسببة للسيناريو الذي يتحقق، أو على أنها نقاط ضعف .
٢,٥,٥ يجب على إدارة قسم أمن المعلومات إجراء تقييم دوري لمخاطر تقنية المعلومات للأصول المتعلقة بتقنية المعلومات (العمليات والأنظمة) وتقديم توصيات لأصحاب المخاطر لتخفيفها والتقليل منها.

٢,٦. الاستجابة لمخاطر تقنية المعلومات (IT Risk Response)

تتمثل الاستجابة للمخاطر في جعل المخاطر المحددة تتماشى مع مستوى المخاطر المقبولة والحد المسموح به للمؤسسة. وبعبارة أخرى، يجب تحديد الاستجابة بحيث يقع أكبر قدر ممكن من المخاطر المتبقية في المستقبل (عادةً ما يعتمد على الميزانيات المتاحة) ضمن حدود المخاطر المقبولة. عندما يُظهر التحليل انحراف المخاطر عن مستويات التحمل المحددة، يجب تحديد الاستجابة. ويمكن أن تكون هذه الاستجابة بأي من الطرق الاربعة الممكنة مثل تجنب المخاطر، والتقليل/ التخفيف من المخاطر ، وتقاسم/ نقل المخاطر ، وقبول المخاطر .
٢,٦,١ يجب على المؤسسة وضع مجموعة من المقاييس لتكون بمثابة مؤشرات للمخاطر. ومن المرجح أن تكون مؤشرات المخاطر ذات التأثير الكبير على الاعمال هي مؤشرات المخاطر الرئيسية (KRIs).

٢,٦,٢ يجب أن تبذل المؤسسة جهدًا لتطبيق وقياس وإعداد تقارير عن المؤشرات المختلفة المتكافئة في الحساسية.
٢,٦,٣ لاختيار المجموعة الصحيحة من مؤشرات المخاطر الرئيسية، يجب على المؤسسة القيام بما يلي:
أ) توفير إنذار مبكر للمخاطر العالية لاتخاذ إجراءات استباقية
ب) توفير مراجعة لأحداث المخاطر التي وقعت
ج) تمكين التوثيق والتحليل لاتجاهاتها.
د) توفير مؤشر على مدى تقبل المخاطر وتحملها والتسامح معها من خلال اعداد المقاييس
ه) زيادة احتمالية تحقيق الأهداف الاستراتيجية .
و) المساعدة في التحسين المستمر لبيئة حوكمة المخاطر وإدارتها. يجب على المؤسسة تحديد الاستجابة للمخاطر لجعل المخاطر تتماشى مع مدى تقبل المخاطر المحددة للمؤسسة بعد تحليل المخاطر .
٢,٦,٤ يجب على المؤسسة تعزيز ممارسات إدارة مخاطر تقنية المعلومات بشكل عام من خلال عمليات كافية لإدارة المخاطر .
٢,٦,٥ يجب على المؤسسة تقديم العديد من التدابير التي تهدف إلى الحد من أي حدث ضار و/أو تأثير الحدث على الأعمال.

التحديد (Identify)

١. إدارة الأصول (Assets Management)

١,١ قبل شراء أي أصول جديدة لتقنية المعلومات، يجب أن تقوم المؤسسة بإجراء تقييم التوافق (مع النظام الحالي) .
١,٢ يجب أن تتوافق جميع عمليات شراء أصول تقنية المعلومات مع سياسة المشتريات الخاصة بالمؤسسة.
١,٣ يجب إسناد كل أصل من أصول تقنية المعلومات إلى أمين (فرد أو كيان) يكون مسؤولاً عن تطوير وصيانة واستخدام وأمن وسلامة ذلك الأصل .
١,٤ يجب تحديد جميع أصول تقنية المعلومات وتسميتها بوضوح. يجب أن تعكس التسمية التصنيف المحدد للأصول .
١,٥ يجب أن تنشئ المؤسسة قائمة جرد لأصول تقنية المعلومات توضح التفاصيل المهمة (على سبيل المثال، المالك، والمسؤول، وتاريخ الشراء، والموقع، ورقم الترخيص، والتهيئة، وما إلى ذلك) .
١,٦ يجب على المؤسسة مراجعة وتحديث قائمة جرد أصول تقنية المعلومات بشكل دوري.
١,٧ يجب توفير الحماية الكافية لأصول أنظمة المعلومات من الوصول غير المصرح به أو إساءة الاستخدام أو التعديل أو الإدراج أو الحذف أو الاستبدال أو الإلغاء أو الإفصاح .
١,٨ يجب على المؤسسة وضع سياسة للتخلص/ اتلاف (Disposal Policy) لغرض حماية أصول نظم المعلومات. يجب إتلاف جميع البيانات الموجودة على المعدات ووسائط التخزين المرتبطة بها أو الكتابة فوقها قبل بيعها أو التخلص منها أو إعادة إصدارها .
١,٩ يجب على المؤسسة توفير إرشادات لاستخدام الأجهزة المحمولة، خاصةً عند لاستخدام في أماكن العمل الخارجية .
١,١٠ يجب على المؤسسة توفير سياسة لإعادة الأصول الخاصة بها من الموظفين/الأطراف الخارجية عند انتهاء خدمتهم أو عقدهم أو اتفاقهم .
١,١١ يجب على المؤسسة الالتزام بشروط جميع تراخيص البرمجيات وعدم استخدام أي برمجيات لم يتم شراؤها بشكل قانوني أو الحصول عليها بطريقة مشروعة .
١,١٢ يجب أن تخضع البرمجيات الخارجية المستخدمة في بيئة الإنتاج/ البيئة الحية لاتفاقية دعم مع البائعين.

١,١٣ يجب على المؤسسة الموافقة على قائمة البرمجيات فقط التي سيتم استخدامها ضمن اي من اجهزة تقنيات المعلومات .
١,١٤ يجب حظر استخدام البرمجيات غير المصرح بها أو المقرصنة بشكل صارم في المؤسسة.

٢. أصول البرمجيات (Software Assets)

٢,١ يجب أن تكون جميع البرمجيات التي يتم شراؤها وتركيبها من قبل المؤسسة حاصلة على تراخيص قانونية ويجب أن تحتفظ الوحدة/الإدارة المعنية في المؤسسة بسجلات لها .
٢,٢ يجب أن تكون هناك بيئة اختبار منفصلة لإجراء اختبار شامل لوظائف البرمجيات قبل التنفيذ .
٢,٣ يجب إجراء اختبار قبول المستخدم (UAT) والتوقيع عليه من قبل وحدات/إدارات الأعمال المعنية قبل بدء التشغيل الفعلي .
٢,٤ يجب مراعاة متطلبات الامتثال التنظيمي اللازمة للإجراءات والممارسات المصرفية والقوانين ذات الصلة لحكومة العراق .
٢,٥ يجب تصعيد أي أخطاء و/أو عيوب ناتجة عن عيوب التصميم إلى مستويات أعلى في مؤسسات موردي البرمجيات في الوقت المناسب .
٢,٦ يجب الحفاظ على اتفاقية الاسناد واستمراريتها مع مزودي البرمجيات والتطبيقات المستخدمة في بيئة الإنتاج مع اتفاقية السرية.

٣. إدارة القدرات (Capacity Management)

الهدف من إدارة القدرات هو ضمان أن تلبي قدرات تقنية المعلومات متطلبات العمل الحالية والمستقبلية بطريقة فعالة من حيث التكلفة .
٣,١ لضمان قدرة أنظمة تقنية المعلومات والبنية التحتية على دعم وظائف الأعمال، يجب على المؤسسة التأكد من مراقبة ومراجعة مؤشرات مثل الأداء والقدرة والاستخدام .
٣,٢ يجب على المؤسسة وضع عمليات مراقبة ووضع حدود مناسبة لتخطيط وتحديد الموارد الإضافية لتلبية المتطلبات التشغيلية ومتطلبات العمل بفعالية.

٤. تصنيف البيانات (Data Classification)

عامة: جميع بيانات ومعلومات المؤسسة التي من المتوقع بشكل معقول ألا يؤدي الإفصاح عنها إلى أي تأثير أو ضرر أو أذى كما هو مذكور في مستويات التصنيف الأعلى يجب أن تصنف على أنها عامة.
مقيدة: جميع بيانات ومعلومات المؤسسة التي يتوقع بشكل معقول أن يؤدي الإفصاح عنها إلى تأثير سلبي على أعمال المؤسسة أو أنشطتها التجارية أو الأفراد، أو المتعلقة بالمعلومات الشخصية للأشخاص المحميين بموجب أي نظام، تصنف على أنها مقيدة.
سري: تصنف جميع بيانات ومعلومات المؤسسة التي يتوقع بشكل معقول أن يؤدي الإفصاح عنها إلى إلحاق ضرر غير مبرر بالمؤسسة، أو الامن والاقتصاد الوطني أو العلاقات الخارجية للبلاد، على أنها سرية.
سري للغاية: تصنف جميع بيانات ومعلومات المؤسسة التي يتوقع بشكل معقول أن يؤدي الإفصاح عنها إلى إلحاق ضرر جسيم وغير مبرر بالأمن القومي أو الاقتصاد الوطني أو العلاقات الخارجية للبلاد على أنها سرية للغاية.

متطلبات الموظفين المصرح لهم بالتعامل مع المعلومات السرّية	
مقيدة	• يجب تصنيف المعلومات المقيدة من قبل موظفي المؤسسة . • يجب على جميع الموظفين المصرح لهم بالتعامل مع المعلومات المقيدة أو ما فوقها حضور جلسات توعية بحماية المعلومات وتصنيفها قبل منحهم التصريح. • يجب تطبيق سياسة المكتب النظيف (Clear Desk Policy). • يجب تطبيق سياسة الشاشات (Clear Screen Policy).
سري	• يجب أن تكون قائمة الموظفين المصرح لهم بالتعامل مع المعلومات السرية تحت هذا المستوى محكمة قدر الإمكان، وأن يتم الاحتفاظ بها وتحديثها بانتظام والموافقة عليها من قبل المؤسسة . • يجب على جميع الموظفين المصرح لهم بالتعامل مع المعلومات السرية تحت هذا المستوى التعهد بحماية المعلومات والتوقيع على بنود عدم الإفصاح .
سري للغاية	• يجب إجراء الفحص المناسب واجراءات التحقق للموظفين المصرح لهم بالتعامل مع المعلومات السرية تحت هذا المستوى وفقًا لسياسة الموارد البشرية للمؤسسة . • يجب الاحتفاظ بسجل يتضمن جميع الموظفين الذين اطلعوا على معلومات سرية تحت هذا المستوى .
متطلبات التعامل مع المعلومات السرية لإنشاء أو معالجة أو طباعة أو نسخ المعلومات السرية	
مقيدة	• لا يسمح بطباعة ونسخ المعلومات المقيدة خارج المؤسسة. • لا يسمح بنسخ المعلومات المقيدة أو جزء منها وإرسالها عبر وسائل التواصل الاجتماعي أو الرسائل الفورية خارج المؤسسة.
سري	لا يُسمح بطباعة ونسخ المعلومات السرية دون الحصول على الموافقات المطلوبة
سري للغاية	يجب تحديد جميع الموظفين المصرح لهم بإنشاء معلومات سرية للغاية أو التعامل معها أو طباعتها أو نسخها
متطلبات تخزين المعلومات السرية	
مقيدة	• يجب ألا يتم تخزين المعلومات المقيدة إلا على أجهزة المؤسسة أو الأجهزة الخارجية المصرح بها من قبل المؤسسة (مثل تلك المستخدمة من قبل أطراف خارجية أو مقدمي الخدمات السحابية). • يجب تشفير وسائط التخزين المتنقلة التي تستضيف المعلومات المصنفة كمعلومات مقيدة.
سري	• يجب تخزين المعلومات السرية تحت هذا المستوى فقط على أصول المعلومات والتقنيات الخاصة بالمؤسسة.

سري للغاية	• يجب دائمًا تشفير المعلومات السرية تحت هذا المستوى عند تخزينها إلكترونيًا. • يجب أن يُسمح باستخدام وسائط التخزين المتنقلة (مثل الأقراص الصلبة الخارجية ووسائط الخزن المحمولة) لتخزين المعلومات السرية تحت هذا المستوى بعد الحصول على الموافقات المناسبة. • لا يجوز تخزين المعلومات السرية تحت هذا المستوى على الخدمات السحابية غير الحكومية.
متطلبات الوصول والوصول عن بُعد للمعلومات السرية	
مقيدة	• يجب تنفيذ ضوابط ومتطلبات الأمن السيبراني بموجب سياسة المؤسسة لإدارة الهوية والوصول إلى المعلومات. • يجب تطبيق ضوابط منع تسريب المعلومات وتنفيذها على المعلومات المقيدة وفقًا لسياسة ومعيار حماية المعلومات والمعلومات الخاصة بالمؤسسة.
سري	• لا يجوز الوصول إلى المعلومات السرية تحت هذا المستوى عن بعد. • يجب تزويد الموظفين بإمكانية الوصول في وقت محدد للتعامل مع المعلومات السرية تحت هذا المستوى.
سري للغاية	• يجب مراجعة الوصول إلى المعلومات السرية تحت هذا المستوى وتوفيرها من خلال موافقة خطية مسبقة. • يجب تقديم الموافقات الخطية المسبقة من قبل المؤسسة أو أي فرد مخول من قبل المؤسسة. • لا يجوز منح الموافقات للأفراد غير العراقيين إلا بموجب استثناء وفقاً للاتفاقيات الدولية بموجب أمر كتابي مبرر من المؤسسة بعد إجراء عمليات التحقق اللازمة.
متطلبات النقل الإلكتروني للمعلومات السرية	
مقيدة	يجب إرسال المعلومات المقيدة التي سيتم تضمينها في رسائل البريد الإلكتروني فقط باستخدام نظام البريد الإلكتروني الخاص بالمؤسسة.
سري	• يجب أن تكون المعلومات السرية التي سيتم إرسالها أو نقلها إلكترونياً عبر قنوات الاتصال (مثل البريد الإلكتروني أو نقل الملفات) مشفرة ومحمية بكلمة سرية، حيث يجب مشاركة كلمة السر على قناة اتصال مختلفة غير البريد الإلكتروني. • يجب ألا تحتوي رسائل البريد الإلكتروني التي تحتوي على معلومات سرية على موضوع يكشف عن محتوى المعلومات أو تصنيفها.
سري للغاية	لا يجوز إرسال المعلومات السرية للغاية أو نقلها إلكترونياً عبر قنوات الاتصال (مثل البريد الإلكتروني أو نقل الملفات أو مشاركة الملفات عبر الإنترنت وغيرها).
متطلبات تدمير المعلومات السرية والتخلص منها	
مقيدة	يجب مسح المعلومات المقيدة من أجهزة التخزين التي سيعاد استخدامها.

سري	• يتم التخلص من أجهزة التخزين التي تتعامل مع المعلومات السرية تحت هذا المستوى عن طريق اتلافها بالكامل. • يجب توثيق أجهزة التخزين التي تتعامل مع المعلومات السرية تحت هذا المستوى والتي سيتم التخلص منها في سجل معتمد وموقع من اللجنة المعنية.
سري للغاية	
متطلبات الاجتماعات التي يتم فيها مناقشة معلومات سرية	
مقيدة	• يتم التخلص من المعلومات المقيدة التي يتم مناقشتها خلال الاجتماعات، بما في ذلك o ملفات العروض التقديمية على أجهزة العرض o الأوراق والملاحظات o المعلومات السرية على لوحات العرض الداخلية
سري	• تُعقد اجتماعات مناقشة المعلومات السرية في غرفة اجتماعات آمنة. • يجب تحديد قائمة بالحضور للاجتماعات التي تعقد لمناقشة المعلومات السرية. • يجب مراجعة امتيازات الاطلاع على المعلومات السرية والتحقق منها للحاضرين في الاجتماعات التي ستتم فيها مناقشة المعلومات السرية. • لا يُسمح للموظفين غير المعنيين بالاجتماع بالدخول إلى غرفة الاجتماعات التي ستتم فيها مناقشة المعلومات السرية
سري للغاية	• يجب تحديد جميع الحاضرين في الاجتماعات التي ستتم فيها مناقشة معلومات سرية للغاية والموافقة عليها. • لا يسمح بدخول جميع الأجهزة التي يمكنها الاتصال بشبكات الاتصالات (مثل شبكة الاتصالات المتنقلة والشبكة اللاسلكية والشبكة المحلية والإنترنت وغيرها) بما في ذلك الأجهزة المحمولة وأجهزة الكمبيوتر المحمولة والهواتف المحمولة والأجهزة الشخصية أو أي أجهزة أخرى متصلة في غرفة الاجتماعات التي ستتم فيها مناقشة معلومات سرية للغاية إلا بعد الحصول على الموافقة المناسبة من المؤسسة. • لا يسمح باستخدام جميع أجهزة التسجيل في غرفة الاجتماعات التي ستتم فيها مناقشة معلومات سرية للغاية إلا بعد الحصول على الموافقة المناسبة من المؤسسة.
متطلبات الكشف عن المعلومات السرية	
مقيدة	لا يجوز الإفصاح عن المعلومات المقيدة إلا بعد الحصول على إذن رسمي من المؤسسة.
سري	

سري للغاية	لا يجوز الإفصاح عن المعلومات السرية تحت هذا المستوى إلا بعد الحصول على الموافقات المناسبة.
متطلبات الإبلاغ عن الخروقات والانتهاكات وتسريب المعلومات السرية	
مقيدة	في حال تم الكشف عن معلومات أو الاشتباه في تسريبها أو إفشائها أو سرقتها أو نشرها ، يتم إبلاغ البنك المركزي العراقي مباشرة من خلال رسالة رسمية أو بريد إلكتروني يوضح فيها وقائع الحادثة، مع تحديد نوع الحدث.
سري	
سري للغاية	في حالة الكشف عن معلومات سرية للغاية أو الاشتباه في تسريبها أو إفشائها أو سرقتها أو نشرها ، يتم إرسال إخطار عاجل وسري بالإضافة إلى خطاب موجه إلى البنك المركزي العراقي يوضح نوع المعلومات السرية التي تم تسريبها.
متطلبات النقل المادي	
مقيدة	يجب تشفير المعلومات المقيدة وتخزينها على ذاكرة فلاش أثناء السفر.
سري	• يجب الحصول على إذن من المؤسسة لنقل المعلومات السرية تحت هذا المستوى أثناء النقل المادي. • يجب التخلص من أجهزة التخزين التي تحتوي على معلومات سرية تحت هذا المستوى والمستخدمة أثناء السفر بشكل كامل وتوثيقها في سجل معتمد وموقع من اللجنة المعنية.
سري للغاية	
متطلبات الأجهزة المحمولة	
مقيدة	• في حالة الحاجة إلى ذلك، يجب تخزين المعلومات السرية تحت هذا المستوى التي يتم حملها على الأجهزة المحمولة أثناء السفر على أجهزة تخزين خارجية (مثل ذاكرة فلاش) وتسجيلها تحت عهدة الموظف.
سري	• لا يجوز توصيل أجهزة التخزين الخارجية التي تحتوي على معلومات سرية تحت هذا المستوى وفتحها باستخدام جهاز عام.
سري للغاية	لا يجوز إنشاء المعلومات السرية للغاية أو نقلها أو معالجتها أو تخزينها على الأجهزة المحمولة

الحماية (Protect)

ستضمن المبادئ التوجيهية المدرجة في الحماية (Protection) تطوير وتنفيذ الضمانات المناسبة لضمان تقديم خدمات البنية التحتية الحيوية.

١. ضوابط الاجهزة الطرفية (Endpoint controls)

تحدد ضوابط الاجهزة الطرفية متطلبات حماية أجهزة المستخدم النهائي والخوادم

١,١. ضوابط أمن الحواسيب المكتبية/والمحمولة (Desktop/Laptop security controls)

١,١,١ يجب توصيل أجهزة الحاسوب بمزودات الطاقة المستمرة "UPS" لمنع الاضرار عن البيانات والمكونات المادية.

١,١,٢ قبل ترك الحاسوب المنضدي أو المحمول دون مراقبة، يجب على المستخدمين تطبيق خاصية "غلق الشاشة- Lock workstation feature". في حال لم يتم تطبيقها، فسيتم غلق الجهاز تلقائيًا وفقًا لسياسة المؤسسة .

١,١,٣ يجب تشفير المعلومات السرّية أو الحساسة المخزونة في أجهزة الحاسوب المحمولة .

١,١,٤ يجب إيقاف تشغيل أجهزة الحاسوب المنضدية و المحمولة والشاشات وما إلى ذلك في نهاية كل يوم عمل .

١,١,٥ يجب تخزين أجهزة الحاسوب المحمولة ووسائط الحاسوب وأي أشكال أخرى من وحدات التخزين التي تحتوي على معلومات حساسة (مثل الأقراص المدمجة (CD) وذاكرة التخزين المحمولة وسائط التخزين المحمولة (فلاش) والأقراص الصلبة الخارجية) في مكان آمن أو خزانة مغلقة في حالة عدم استخدامها .

١,١,٦ يجب التحكم في الوصول إلى منافذ يو إس بي (USB) لأجهزة الحاسوب المنضدية/المحمولة.

١,١,٧ يجب تخزين وسائط تخزين المعلومات الأخرى التي تحتوي على بيانات سرية مثل الورق والملفات والأشرطة وما إلى ذلك في مكان آمن أو خزانة مغلقة في حالة عدم استخدامها .

١,١,٨ يجب على المستخدمين الأفراد عدم تثبيت أو تحميل تطبيقات البرامج و/أو الملفات القابلة للتنفيذ على أي حاسوب منضدي أو محمول دون إذن مسبق .

١,١,٩ لا يجوز لمستخدمي الحواسيب المنضدية والمحمولة كتابة أو تجميع أو نسخ أو نشر أو تنفيذ أو محاولة إدخال أي رمز حاسوبي مصمم للنسخ الذاتي أو الإضرار أو تقليل أداء أي نظام حاسوبي (مثل الفيروسات أو البرامجيات الضارة او غيرها) .

١,١,١٠ يجب الإبلاغ عن أي نوع من الفيروسات على الفور .

١,١,١١ يجب تحديد هوية المستخدم (الهوية) والمصادقة (كلمة المرور) للدخول إلى جميع أجهزة الحاسوب المنضدية والمحمولة عند تشغيلها أو إعادة تشغيلها .

١,١,١٢ يجب تثبيت برنامج قياسي ومعتمد للكشف عن الفيروسات على جميع أجهزة الحاسوب المنضدية والمحمولة وتهيئته لفحص الملفات عند قراءتها والمسح الروتيني للنظام لاكتشاف الفيروسات.

١,١,١٣ يجب تهيئة أجهزة الحاسوب المنضدية والمحمولة لتسجيل جميع الأحداث الهامة ذات الصلة بأمن الحاسوب. (على سبيل المثال، تخمين كلمة المرور أو محاولات الدخول غير المصرح بها أو التعديلات على التطبيقات أو برمجيات النظام) .

١,١,١٤ يجب وضع جميع أجهزة الحاسوب فوق مستوى الأرض وبعيدًا عن النوافذ.

١,٢. ضوابط أمن الخوادم (Server Security controls)

١,٢,١ يجب أن يكون للمستخدمين تفويض محدد للوصول إلى الخوادم مع مجموعة محددة من الامتيازات .

١,٢,٢ يجب استخدام آلية مصادقة إضافية للتحكم في وصول المستخدمين عن بعد .

١,٢,٣ تنتهي صلاحية جلسة العمل غير النشطة بعد فترة محددة من عدم النشاط .

١,٢,٤ يجب تسجيل أنشطة مديري النظام، يجوز للخوادم التي تحتوي على بيانات حساسة وسرية ارسال سجلات النشاط إلى مضيف سجل مركزي .

١,٢,٥ يجب على المؤسسة توفير خوادم اختبار لتوفير منصة لاختبار إعدادات التهيئة والتحديثات الجديدة وحزم الخدمات قبل تطبيقها على نظام بيئة الإنتاج (الحية).

١,٢,٦ يجب على المؤسسة ضمان أمن عملية مشاركة الملفات، يجب تعطيل مشاركة الملفات والطباعة إذا لم تكن مطلوبة أو إبقائها عند الحد الأدنى حيثما أمكن .
١,٢,٧ يجب تعطيل جميع الخدمات غير الضرورية التي تعمل في خادم بيئة الإنتاج (الحية). يجب عدم تشغيل أي خدمات جديدة على خادم بيئة الإنتاج دون اختبار مسبق .
١,٢,٨ يجب إلغاء تثبيت جميع البرامج غير الضرورية من خوادم بيئة الإنتاج.
١,٢,٩ في حالة البيئات الافتراضية (Virtualization):
أ) يجب أن تخطط المؤسسة لوضع حد لاستخدام الموارد (على سبيل المثال، المعالجات والذاكرة ومساحة القرص وواجهات الشبكة الافتراضية) لكل بيئة افتراضية (VM) .
ب) يجب تحديث انظمة التشغيل للخوادم الافتراضية (Host and Guest Operating Systems) بالتحديثات الأمنية الجديدة/والمطلوبة والتحديثات الاخرى عند الحاجة، يجب أيضاً تطبيق متطلبات التحديث على برامج البيئات الافتراضية .
ج) يجب إجراء نسخ احتياطي للخوادم الافتراضية بانتظام مثل الخوادم الفعلية .
د) يجب على المؤسسة التأكد من أن الخوادم الافتراضية (Host and Guest) يستخدمون توقيتاً متزامناً .
ه) يجب عدم السماح بمشاركة الملفات بين انظمة التشغيل للخوادم الافتراضية (Host and Guest Operating Systems)، إذا لم يكن ذلك مطلوباً.

٢. ضوابط مركز البيانات (Data Center controls)

نظرًا لأن الأنظمة والبيانات الهامة للمؤسسة تتركز وتوجد في مركز البيانات ، فمن المهم أن يكون مركز البيانات مرنًا ومؤمنًا ماديًا من التهديدات الداخلية والخارجية.

٢,١. الأمن المادي (Physical Security)

٢,١,١ يجب تطبيق الأمن المادي على منطقة معالجة المعلومات أو مركز البيانات. ويجب أن تكون منطقة مركز البيانات مقيدة ويحظر الدخول غير المصرح به إليها بشكل صارم. يجب على المؤسسة أن تحصر الوصول إلى مركز البيانات على الموظفين المصرح لهم فقط. يجب أن تمنح المؤسسة حق الوصول إلى مركز البيانات فقط على أساس الحاجة. يجب إلغاء الدخول الفعلي للموظفين إلى مركز البيانات على الفور إذا لم تعد هناك حاجة لذلك .
٢,١,٢ تطبق إجراءات التصريح بالدخول بصرامة على البائعين ومقدمي الخدمات وموظفي الدعم وأطقم التنظيف. يجب أن تضمن المؤسسة أن يكون الزوار مصحوبين دائمًا بموظف مخول أثناء وجودهم في مركز البيانات .
٢,١,٣ يجب الاحتفاظ بقائمة تصاريح الدخول ومراجعتها بشكل دوري للشخص المصرح له بالدخول إلى مركز البيانات.
٢,١,٤ يجب تسجيل جميع عمليات الدخول المادي إلى المناطق الحساسة مع الغرض من الدخول إلى مركز البيانات .
٢,١,٥ يجب على المؤسسة التأكد من أن محيط مركز البيانات والمنشأة وغرفة المعدات مؤمنة ومراقبة ماديًا. يجب على المؤسسة توظيف الضوابط الامنية المادية والبشرية والإجرائية على مدار ٢٤ ساعة مثل استخدام حراس الأمن ونظام الدخول بالبطاقات، نظام المراقبة عند الحاجة .
٢,١,٦ يجب أن يكون باب خروج الطوارئ متاحًا .
٢,١,٧ يجب أن يكون لمركز البيانات أمين أو مدير معين مسؤول عن توفير التخويل وضمان الامتثال للسياسة .

٢,١,٨ يجب أن يحتفظ المدير أو من يفوضه بقائمة جرد لجميع المعدات التقنية والمعدات المرتبطة بها والمواد المستهلكة الموجودة في مركز البيانات .
٢,١,٩ عندما يتم تشغيل مركز البيانات من قبل مورد خدمات خارجي، يجب أن يشير العقد المبرم بين المؤسسة والمورد إلى ضرورة الامتثال لجميع متطلبات السياسة المتعلقة بالأمن المادي، وتحتفظ المؤسسة بالحق في مراجعة حالة الأمن المادي في أي وقت.
٢,١,١٠ حيثما يتم تشغيل مركز الخدمات من قبل مورد خدمات خارجي، تقع مسؤولية الأمن المادي على عاتق المورد، ولكن يجب مراجعة الوصول إلى هذه المرافق المخصصة والتصريح بها من قبل المؤسسة.

٢,٢. الأمن البيئي (Environmental Security)

٢,٢,١ يجب تصميم وتطبيق حماية مركز البيانات من مخاطر الأضرار الناجمة عن الحرائق والفيضانات والانفجارات وغيرها من أشكال الكوارث. لا يُنصح بتشييد مركز البيانات وموقع التعافي من الكوارث في مبنى متعدد المستأجرين .
٢,٢,٢ يجب توثيق تصميم مخطط مركز البيانات بما في ذلك مصدر الطاقة واتصال الشبكة بشكل صحيح .
٢,٢,٣ يجب فصل بيئة التطوير والاختبار عن بيئة الإنتاج .
٢,٢,٤ يجب عمل قنوات منفصلة لكابلات البيانات والطاقة للحماية من التداخل أو أي نوع من التلف في مركز البيانات .
٢,٢,٥ يجب وضع أجهزة كشف المياه أسفل الأرضية المرتفعة إذا كانت مرتفعة .
٢,٢,٦ يجب عدم السماح بتخزين أي ملحقات أو أجهزة غير مرتبطة بمركز البيانات والاجهزة المتوقفة عن العمل في مركز البيانات. يجب وضع مخزن منفصل لحفظ جميع أنواع معدات تقنية المعلومات غير المستخدمة والاحتياطية.
٢,٢,٧ يجب تركيب منظومة المراقبة من خلال الكاميرات (Closed Circuit Television / CCTV) في مواقع مناسبة في جميع الاتجاهات للمراقبة الصحيحة.
٢,٢,٨ يجب وضع لافتة "ممنوع الأكل أو الشرب أو التدخين ."
٢,٢,٩ يجب توفير مركبات مخصصة للمؤسسة لحالات الطوارىء دائمًا في الموقع. يجب تجنب استخدام وسائل النقل العام أثناء نقل المعدات الهامة خارج مقر المؤسسة لتجنب خطر حدوث أي طارئ .
٢,٢,١٠ يجب أن يكون لمركز البيانات خط هاتف مخصص للاتصال .
٢,٢,١١ يجب أن تكون العناوين وأرقام الهواتف أو الهواتف المحمولة لجميع الأشخاص الذين يمكن الاتصال بهم (مثل خدمة الإطفاء، ومركز الشرطة، ومقدمي الخدمات، والبائعين، وجميع موظفي تقنية المعلومات) متاحة لتلبية أي ضرورة طارئة.
٢,٢,١٢ يجب فصل نظام الإمداد بالطاقة ووحدات الدعم الأخرى عن موقع الإنتاج ووضعها في منطقة آمنة للحد من المخاطر الناجمة عن التهديدات البيئية .
٢,٢,١٣ يجب أن يكون مصدر إمداد الطاقة من المصدر (الموزع الرئيسي أو المولد) مخصصاً لمركز البيانات. يجب تقييد المنافذ الكهربائية من مصادر الطاقة هذه لأي أجهزة أخرى ومراقبتها لتجنب مخاطر التحميل الزائد .
٢,٢,١٤ يجب تركيب وحدات السيطرة البيئية التالية :
أ) إمدادات الطاقة غير المنقطعة (UPS) مع وحدات احتياطية
ب) مصدر طاقة احتياطي
ج) أجهزة قياس درجة الحرارة والرطوبة
د) تحذيرات تسرب المياه

هـ) مكيفات الهواء مع وحدات احتياطية. يجب تنفيذ المعايير القياسية لمكيفات الهواء لتجنب تسرب المياه من المكيفات.
و) مفاتيح قطع التيار الكهربائي (Emergency power cut-off switches) في حالات الطوارئ عند الحاجة
ز) ترتيبات الإضاءة في حالات الطوارئ
ح) يجب اختبار أجهزة إزالة الرطوبة للتحكم في الرطوبة بانتظام
ط) يجب الاتفاق على عقد خدمة الصيانة على مدار الاسبوع ٧/٢٤.

٢,٣. الوقاية من الحرائق (Fire Prevention)

٢,٣,١ يجب أن يكون جدار وسقف وباب مركز البيانات مقاومًا للحريق .
٢,٣,٢ يجب تركيب معدات إخماد الحرائق واختبارها بشكل دوري .
٢,٣,٣ يجب تركيب نظام إنذار آلي للحريق/الدخان واختباره بشكل دوري .
٢,٣,٤ يجب أن يكون هناك كاشف للحريق أسفل الأرضية المرتفعة إذا كانت مرتفعة وفوق السقف المستعار.
٢,٣,٥ يجب الحفاظ على جودة الكابلات الكهربائية وكابلات البيانات في مركز البيانات وإخفاؤها .
٢,٣,٦ يجب عدم السماح بتخزين المواد القابلة للاحتراق مثل الورق والأشياء الخشبية والبلاستيك وغيرها في مركز البيانات.

٢,٤. ضوابط قاعات الخوادم/ والشبكات/ وحوامل الاجهزة (Servers/Network Room/ Rack (Controls)

٢,٤,١ يجب أن يكون لحامل الاجهزة ابواب زجاجية مزودة بقفل ومفتاح تحت إشراف موظف مسؤول .
٢,٤,٢ يجب تقييد الوصول المادي، ويجب وجود سجل للزوار والاحتفاظ به لغرفة الخوادم .
٢,٤,٣ يجب الاحتفاظ بقائمة تصاريح الدخول ومراجعتها بشكل منتظم .
٢,٤,٤ يجب أن يكون هناك اجراءات لاستبدال الخوادم وأجهزة الشبكة في أقصر وقت ممكن في حالة حدوث أي كارثة .
٢,٤,٥ يجب أن يكون هناك مولد طاقة لمواصلة العمليات في حالة انقطاع التيار الكهربائي .
٢,٤,٦ يجب أن يكون مولد الطاقة غير المنقطعة (UPS) موجودًا لتوفير إمدادات الطاقة دون انقطاع للخوادم والأجهزة المطلوبة .
٢,٤,٧ يجب إيلاء الاهتمام المناسب لتجنب التحميل الزائد على المنافذ الكهربائية المزودة للعديد من الأجهزة .
٢,٤,٨ يجب توفير قناة للسماح بتوصيل كابلات إمدادات الطاقة وكابلات البيانات في وضع مرتب وآمن .
٢,٤,٩ يجب أن تكون عناوين وأرقام هواتف جميع الأشخاص الذين يمكن الاتصال بهم (مثل خدمة الإطفاء، ومركز الشرطة، ومقدمي الخدمات، والبائعين، وجميع موظفي تقنية المعلومات/المسؤولين) متاحة للتصدي لأي طارئ .
٢,٤,١٠ يجب وضع طفاية حريق في منطقة خارجية مرئية في غرفة الخوادم. يجب صيانتها وفحصها سنوياً.

٣. إدارة أمن الشبكات (Network security management)

٣,١. إرشادات التحكم في الشبكة المحلية (Local Area Network Control Guidelines)

٣,١,١ يجب على المؤسسة وضع معايير أساسية لضمان أمن أنظمة التشغيل وقواعد البيانات ومعدات الشبكة والأجهزة المحمولة التي يجب أن تتوافق مع سياسة المؤسسة .
٣,١,٢ يجب على المؤسسة إجراء فحوصات تنفيذية منتظمة لضمان تطبيق المعايير الأساسية بشكل موحد، واكتشاف حالات عدم الامتثال ورفعها للتحقيق فيها .

٣,١,٣ يجب تنفيذ تصميم الشبكة وتهيئتها الأمنية بموجب خطة موثقة. يجب أن تكون هناك مناطق أمنية (Security Zones) مختلفة محددة في تصميم الشبكة .
٣,١,٤ يجب أن تكون جميع أنواع الكابلات بما في ذلك كابلات UTP ، والألياف الضوئية، والطاقة تحمل علامات مناسبة لأعمال الصيانة التصحيحية أو الوقائية .
٣,١,٥ يجب على المؤسسة ضمان الأمن المادي لجميع معدات الشبكة .
٣,١,٦ يجب فصل مجموعات خدمات المعلومات والمستخدمين ونظم المعلومات في الشبكات، على سبيل المثال، الشبكة المحلية الافتراضية Vlan(s).
٣,١,٧ يجب التحكم بصرامة في الوصول غير المصرح به والتغيير. يجب وضع آلية لتشفير وفك تشفير البيانات الحساسة التي تنتقل عبر الشبكة الخارجية (WAN) أو الشبكة العامة .
٣,١,٨ يجب على المؤسسة تركيب أجهزة أمن الشبكة، مثل جدران الحماية وكذلك أنظمة كشف ومنع التطفل/ التدخل في المستويات الحرجة من البنية التحتية لتقنية المعلومات لحماية محيط الشبكة .
٣,١,٩ يجب على المؤسسة نشر جدران الحماية وغيرها من التدابير/الطبقات الأمنية الأخرى، ضمن الشبكات الداخلية للحد من تأثير التعرضات الأمنية الناشئة من طرف خارجي أو من أنظمة خارجية، وكذلك من الشبكة الداخلية الموثوقة .
٣,١,١٠ يجب تمكين خاصية تسجيل الدخول الآمن (على سبيل المثال SSH) في أجهزة الشبكة لأغراض الإدارة عن بعد. يجب تعطيل أي خيار تسجيل دخول غير مشفر (على سبيل المثال TELNET).
٣,١,١١ يجب أن تقوم المؤسسة بعمل نسخة احتياطية ومراجعة الادوار على أجهزة أمن الشبكة بشكل منتظم لتحديد ما إذا كانت هذه الادوار مناسبة وذات صلة .
٣,١,١٢ يجب على المؤسسة إنشاء قنوات اتصال احتياطية للاتصالات الخارجية (WAN Connectivity) .
٣,١,١٣ يجب أن تكون المؤسسة التي تنشر شبكات محلية لاسلكية (WLAN) داخلها على دراية بالمخاطر المرتبطة بهذه البيئة. يجب تنفيذ بروتوكولات الاتصال الآمنة لعمليات الإرسال بين نقاط الوصول ومستخدمين الشبكات اللاسلكية لتأمين الشبكة من الوصول غير المصرح به.
٣,١,١٤ قد يتم إنشاء خوادم تسجيل الاحداث (SYSLOG servers) اعتماداً على حجم الشبكة لمراقبة السجلات/ الاحداث المتكونة من الاجهزة الشبكية.
٣,١,١٥ يمكن إنشاء خوادم المصادقة والتخويل والمراقبة (AAA Servers) اعتماداً على حجم الشبكة لإدارة أجهزة الشبكة بفعالية .
٣,١,١٦ يجب تنفيذ قوائم التحكم في الوصول المستندة إلى الادوار و/أو قوائم التحكم في الوصول المستندة إلى الوقت (ACLs) في أجهزة التوجيه للتحكم في تدفق البيانات ضمن الشبكة.
٣,١,١٧ يمكن تطبيق نظام المراقبة في الوقت الحقيقي لإدارة البنية التحتية لمراقبة جميع معدات الشبكة والخوادم .
٣,١,١٨ يجب تقييد وتأمين اتصال الحاسوب المحمول الشخصي بشبكة المكتب أو أي اجهزة لاسلكية شخصية مع الحاسوب المحمول/الحاسوب المنضدي الخاص بالمؤسسة.
٣,١,١٩ يجب على المؤسسة تغيير جميع كلمات المرور الافتراضية لأجهزة الشبكة .
٣,١,٢٠ يجب إغلاق جميع المنافذ غير المستخدمة لأجهزة الوصول الشبكية .
٣,١,٢١ يجب ضمان الإدارة القائمة على الأدوار للخوادم.

٤. معاملات أجهزة الصراف الآلي واجهزة نقاط البيع (ATM/POS Transactions)

لقد سهلت أجهزة الصراف الآلي (ATM) وأجهزة نقاط البيع (POS) لحاملي البطاقات إمكانية سحب النقود بسهولة وكذلك سداد المدفوعات للتجار ومؤسسات الفوترة. ومع ذلك، فإن هذه الأنظمة تعتبر أهدافًا تُرتكب فيها

هجمات نسخ/قراءة البطاقات. ولتأمين ثقة المستهلك في استخدام هذه الأنظمة، يجب على المؤسسة النظر في وضع التدابير التالية لمواجهة هجمات المحتالين على أجهزة الصراف الآلي وأجهزة نقاط البيع:

٤,١ يجب على المؤسسة تركيب حلول مضادة للنسخ والقراءة السريعة (anti-skimming solutions) على أجهزة الصراف الآلي للكشف عن وجود أجهزة غير معروفة موضوعة فوق أو بالقرب من فتحة إدخال البطاقة .

٤,٢ يجب على المؤسسة تركيب آليات الكشف وإرسال تنبيهات إلى الموظفين المناسبين لمتابعة الاستجابة والإجراءات .

٤,٣ يجب على المؤسسة تركيب لوحات مفاتيح مقاومة للتلاعب (tamper-resistant keypads).

٤,٤ يجب على المؤسسة تنفيذ التدابير المناسبة لمنع رصد أرقام التعريف الشخصي للعملاء (prevent shoulder surfing of customers' PINs).

٤,٥ يمكن للمؤسسة تطبيق تقنية استشعار أوردة الأصابع البيومترية (biometric finger vein sensing technology) لمنع الحصول على رقم التعريف الشخصي (PIN compromise).

٤,٦ يجب على المؤسسة إجراء مراقبة فيديوية للأنشطة لمدة ٢٤ ساعة على هذه الآلات والحفاظ على جودة لقطات كاميرات المراقبة والاحتفاظ بها لمدة سنة واحدة على الأقل .

٤,٧ يجب على المؤسسة التحقق من تطبيق تدابير أمنية مادية كافية في أجهزة الصراف الآلي .

٤,٨ يجب على المؤسسة فحص جميع أجهزة الصراف الآلي / نقاط البيع بشكل متكرر للتأكد من تطبيق الممارسات القياسية (أي الأمن البيئي لأجهزة الصراف الآلي، وأجهزة منع النسخ في أجهزة الصراف الآلي، والعبث بأجهزة نقاط البيع، وما إلى ذلك) مع الامتثال اللازم. يجب الاحتفاظ بسجل التحقق مركزياً وضمن موقع المؤسسة .

٤,٩ يجب على المؤسسة مراقبة أنشطة موردي تجديد النقد من الطرف الخارجي باستمرار وزيارة مراكز الفرز النقدي من الطرف الخارجي بانتظام.

٤,١٠ تقوم المؤسسة بتدريب التجار وتزويدهم بالوثائق الضرورية عن الممارسات الأمنية (مثل التحقق من التوقيع، ومحاولة العبث بالجهاز أو استبدال الجهاز، وتغيير كلمة المرور الافتراضية، وما إلى ذلك) الواجب اتباعها في التعامل مع أجهزة نقاط البيع (POS).

٤,١١ يجب على المؤسسة توعية عملائها بالتدابير الأمنية التي وضعتها والتي يجب على العملاء الالتزام بها في معاملات أجهزة الصراف الآلي ونقاط البيع.

٥. الحماية من الشفرات الخبيثة (Malicious Code Protection)

٥,١ يجب حماية بيئة المؤسسة بما في ذلك الخوادم والاجهزة الطرفية من البرمجيات الخبيثة من خلال ضمان تثبيت حزم حماية معتمدة للاجهزة الطرفية .

٥,٢ يجب أن يكون المستخدمون على علم بالترتيبات اللازمة لمنع وكشف إدخال البرمجيات الخبيثة .

٥,٣ يجب فحص البرمجيات والبيانات الداعمة لأنشطة العمل الحرجة أو مسحها بانتظام لتحديد الشفرات الضارة المحتملة .

٥,٤ يجب فحص الملفات الواردة على وسائط إلكترونية وشبكات غير معروفة/ غير مؤكدة المصدر للتأكد من عدم وجود برمجيات خبيثة قبل استخدامها.

٥,٥ يجب فحص مرفقات البريد الإلكتروني للتأكد من خلوها من الشفرات الخبيثة قبل استخدامها .

٥,٦ يجب تحديث حزمة مكافحة الفيروسات بأحدث ملف تعريف للفيروسات باستخدام عملية آلية وفي الوقت المناسب .

٥,٧ يجب أن تحصل جميع أجهزة الحاسوب في الشبكة على توقيع محدّث لبرنامج مكافحة الفيروسات تلقائياً من الخادم المخصص لذلك.

٥,٨ يجب تمكين وضع الحماية التلقائية من الفيروسات لفحص وحدات الخزن أو الأقراص المدمجة أو الوسائط الأخرى بحثاً عن الفيروسات.
٥,٩ خدعة فيروس الحاسوب (computer virus hoax) هي رسالة تحذر المستلمين من فيروس حاسوب غير موجود. وعادة ما تكون الرسالة عبارة عن سلسلة رسائل بريد إلكتروني متسلسلة تطلب من المتلقين إعادة توجيهها إلى كل من يعرفونه. يجب أن يكون الموظفون على دراية بمشكلة الفيروسات الخادعة ويجب عليهم عدم إعادة توجيه مثل هذه الإنذارات بالفيروسات.
٥,١٠ العمليات التنظيمية لإدارة الهجمات من الشفرات الخبيثة يجب ان تتضمن إجراءات للإبلاغ عن الهجمات والتعافي منها .
٥,١١ يمكن للمؤسسة تنظيم برنامج توعية للمستخدمين النهائيين حول فيروسات الحاسوب وآلية الوقاية منها.

٦. إدارة الوصول إلى الإنترنت (Internet Access Management)

٦,١ يجب توفير الوصول إلى الإنترنت للموظفين وفقاً لسياسة إدارة الوصول إلى الإنترنت المعتمدة .
٦,٢ يجب أن يكون الوصول إلى الإنترنت واستخدامه من مباني المؤسسة آمنًا ويجب ألا يعرّض أمن المعلومات الخاصة بالمؤسسة للخطر .
٦,٣ يجب توجيه الوصول إلى الإنترنت من مباني المؤسسة وأنظمتها من خلال بوابات آمنة .
٦,٤ يحظر أي اتصال محلي مباشر بالإنترنت من مباني المؤسسة أو أنظمتها، بما في ذلك أجهزة الحاسوب المنضدية و المحمولة، ما لم يوافق أمن المعلومات على ذلك .
٦,٥ يحظر على الموظفين إنشاء اتصال خاص بهم بالإنترنت باستخدام أنظمة المؤسسة أو مبانيها.
٦,٦ يجب ألا يستخدم الوصول إلى الإنترنت الذي توفره المؤسسة في إجراء أي نشاط تجاري غير عائد لها، يجب عدم إجراء مصالح تجارية شخصية للموظفين أو غيرهم .
٦,٧ يجب عدم استخدام الوصول إلى الإنترنت الذي توفره المؤسسة في أي نشاط يخالف عن علم أي قانون أو قانون جنائي أو مدني. وسيؤدي أي نشاط من هذا القبيل إلى اتخاذ إجراءات انضباطية بحق الموظفين المعنيين .
٦,٨ يجب أن تخضع جميع التطبيقات والأنظمة التي تتطلب اتصالاً بالإنترنت أو شبكات الطرف الخارجي والشبكات العامة لتحليل رسمي للمخاطر أثناء التطوير وقبل الاستخدام في بيئة الانتاج ويجب تنفيذ جميع آليات الأمن المطلوبة .

٧. إدارة البريد الإلكتروني (Email Management)

٧,١ يجب استخدام نظام البريد الإلكتروني وفقاً لسياسة المؤسسة.
٧,٢ لا يمكن الوصول إلى نظام البريد الإلكتروني إلا من خلال طلب رسمي .
٧,٣ لا يمكن استخدام البريد الإلكتروني لإيصال المعلومات السرية إلى أطراف خارجية إلا إذا كان مشفراً باستخدام وسائل التشفير المعتمدة .
٧,٤ يجب على الموظفين مراعاة سرية وحساسية جميع محتويات البريد الإلكتروني، قبل إعادة توجيه البريد الإلكتروني أو الرد على الأطراف الخارجية .
٧,٥ يجب ألا تكون المعلومات المرسلة عبر البريد الإلكتروني تشهيرية أو مسيئة أو تنطوي على أي شكل من أشكال الإساءة العنصرية أو تضر بسمعة المؤسسة أو تحتوي على أي مواد تضر بالموظفين أو العملاء أو المنافسين أو غيرهم. ومن المحتمل أن يؤدي النقل المتعمد لأي مواد من هذا القبيل إلى اتخاذ إجراءات انضباطية.
٧,٦ يتم توفير نظام البريد الإلكتروني للمؤسسة بشكل أساسي لأغراض العمل، لا يُسمح بالاستخدام الشخصي لنظام البريد الإلكتروني للمؤسسة إلا بموجب تقدير الإدارة ويتطلب إذنًا مناسبًا؛ ويجوز سحب هذا الاستخدام الشخصي أو تقييده في أي وقت .

٧,٧ يجب عدم استخدام عنوان البريد الإلكتروني الخاص بالمؤسسة في أي شبكات اجتماعية أو مدونات أو مجموعات أو منتديات أو ما إلى ذلك ما لم يكن هناك موافقة الإدارة .
٧,٨ يجب أن تحتوي جميع رسائل البريد الإلكتروني المرسلة من المؤسسة إلى نطاقات البريد الإلكتروني الخارجية على إخلاء مسؤولية ينص على حماية سرية محتوى البريد الإلكتروني .
٧,٩ يجب على الإدارة المعنية إجراء مراجعة ومراقبة منتظمة لخدمات البريد الإلكتروني .
٧,١٠ يجب على الموظفين توخي الحذر عند فتح مرفقات البريد الإلكتروني إذا كان المرسل غير معروف.

٨. الهوية ومراقبة الوصول إلى انظمة المعلومات (Identity and Access Control of (Information Systems

لا تمنح المؤسسة حقوق الوصول وامتيازات النظام إلا على أساس المسؤولية الوظيفية. ويجب على المؤسسة التحقق من عدم تمكين أي شخص بحكم الرتبة أو المنصب بأي حق جوهري في الوصول إلى البيانات السرية أو التطبيقات أو موارد النظام أو المرافق لأغراض مشروعة.

٨,١. إدارة الوصول للمستخدم (User Access Management)

٨,١,١ يجب على المؤسسة أن تمنح المستخدم حق الوصول إلى أنظمة وشبكات تقنية المعلومات فقط على أساس الحاجة إلى الاستخدام وفي الفترة التي يكون فيها الوصول مطلوبًا .
٨,١,٢ يجب على المؤسسة أن تراقب عن كثب غير الموظفين (المتعاقدين أو الخارجيين أو كوادر الموردين) فيما يتعلق بقيود الوصول .
٨,١,٣ يجب أن يكون لكل مستخدم معرف مستخدم فريد وكلمة مرور صالحة .
٨,١,٤ يجب أن تكون استمارة معرف المستخدم مع امتيازات الوصول معتمدة وموافق عليها حسب الأصول من الجهة المختصة .
٨,١,٥ يجب تعطيل وصول المستخدم في محاولات الدخول غير الناجحة .
٨,١,٦ يجب أن يتم تحديث امتيازات وصول المستخدم باستمرار مع تغيير حالته الوظيفية .
٨,١,٧ يجب على المؤسسة التأكد من أن سجلات دخول المستخدم محددة بشكل فريد ومسجلة لأغراض التدقيق والمراجعة .
٨,١,٨ يجب على المؤسسة إجراء مراجعات منتظمة لامتيازات وصول المستخدم للتحقق من منح الامتيازات بشكل مناسب.

٨,٢. إدارة كلمات المرور (Password Management)

٨,٢,١ يجب على المؤسسة فرض ضوابط قوية لكلمات المرور على دخول المستخدمين .
٨,٢,٢ يجب أن تتضمن ضوابط كلمة المرور تغيير كلمة المرور عند تسجيل الدخول لأول مرة .
٨,٢,٣ يجب أن تضمن عوامل تعريف كلمة المرور الحفاظ على الحد الأدنى لطول كلمة المرور وفقًا لسياسة المؤسسة (٨ أحرف على الأقل) .
٨,٢,٤ يجب أن تكون كلمة المرور مزيجًا من ثلاثة على الأقل من المعايير المذكورة مثل الأحرف الكبيرة والصغيرة والأحرف الخاصة والأرقام .
٨,٢,٥ يجب ألا تزيد مدة الصلاحية القصوى لكلمة المرور عن عدد الأيام المسموح بها في سياسة المؤسسة (٩٠ يومًا كحد أقصى).

٨,٢,٦ يجب تحديد عوامل للتحكم في العدد الأقصى لمحاولات تسجيل الدخول غير الصالحة بشكل صحيح في النظام وفقًا لسياسة المؤسسة (بحد أقصى ٣ مرات متتالية) .
٨,٢,٧ يجب تمكين صيانة سجل كلمات المرور في النظام للسماح باستخدام نفس كلمات المرور مرة أخرى بعد ثلاث (٣) مرات على الأقل .
٨,٢,٨ يجب الاحتفاظ بكلمات المرور الإدارية لنظام التشغيل وقاعدة البيانات وتطبيقات الأعمال في مكان آمن مع مظروف مغلق .
٨,٢,٩ يجب على المؤسسة إلغاء دخول الموظفين عند التقاعد أو الاستقالة أو إنهاء الوظيفة.

٨,٣. التحكم في ادخال البيانات (Data Input Control)

٨,٣,١ يجب أن يتم تحديد فترة انتهاء وقت الجلسة للمستخدمين وفقًا لسياسة المؤسسة.
٨,٣,٢ يجب تنفيذ الجدول الزمني لوقت تشغيل مدخلات المستخدمين للتطبيقات المصرفية وفقًا للوائح التنظيمية ما لم يسمح بخلاف ذلك من الجهة المختصة .
٨,٣,٣ يجب الاحتفاظ بسجل تدقيق مع معرف المستخدم والطابع الزمني للتاريخ لإدخال البيانات وحذفها وتعديلها .
٨,٣,٤ يجب ألا تسمح البرمجيات لنفس المستخدم بأن يكون مدخلاً ومدققًا لنفس المعاملة، ما لم تسمح الجهة المختصة بخلاف ذلك في الحالات الحرجة.
٨,٣,٥ يجب الحصول على موافقة الإدارة لتفويض الجهة .
٨,٣,٦ يجب تقييد الوصول إلى البيانات والحقول الحساسة للتطبيقات المصرفية.

٨,٤. إدارة امتيازات الوصول (Privileged Access Management- PAM)

يعتمد أمن المعلومات في نهاية المطاف على الثقة في مجموعة صغيرة من الموظفين المهرة الذين يجب أن يخضعوا لضوابط وموازين مناسبة. ويجب أن تخضع مهامهم ووصولهم إلى موارد النظام للتدقيق .
٨,٤,١ يجب أن تطبق المؤسسة معايير اختيار صارمة وفحص شامل عند تعيين الموظفين في العمليات الحيوية والوظائف الأمنية .
٨,٤,٢ يتمتع جميع مديري النظام ومسؤولي أمن تقنية المعلومات والمبرمجين والموظفين الذين يقومون بعمليات حرجة بامتياز الوصول، ويمتلكون دائمًا القدرة على إلحاق أضرار جسيمة بالأنظمة الحيوية. يجب أن تتبنى المؤسسة الضوابط والممارسات الأمنية التالية للمستخدمين المميزين:
أ) تطبيق آليات مصادقة قوية .
ب) تطبيق ضوابط قوية على الوصول عن بعد .
ج) تقييد عدد المستخدمين المميزين .
د) منح حق الدخول المميز على أساس "الحاجة إلى الدخول ."
ه) مراجعة أنشطة المستخدمين المميزين في الوقت المناسب .
و) حظر مشاركة الحسابات المميزة.

٩. إدارة التحديثات (Patch Management)

٩,١ يجب على المؤسسة وضع إجراءات إدارة التحديث والتأكد من أن إجراءات إدارة التحديثات الأمنية تشمل تحديد وتصنيف وترتيب أولويات التحديثات الأمنية. ولتنفيذ التحديثات الأمنية في الوقت المناسب، يجب على المؤسسة تحديد الإطار الزمني لتنفيذ كل فئة من التحديثات الأمنية .
٩,١ يجب على المؤسسة إجراء اختبار دقيق للتحديثات الأمنية قبل تنفيذها في بيئة الإنتاج.

١٠. إدارة تقديم خدمات تقنية المعلومات (IT Service Delivery Management)

تغطي إدارة خدمات تقنية المعلومات ديناميكيات إدارة العمليات التقنية التي تشمل إدارة القدرات وإدارة الطلبات وإدارة التغيير وإدارة الحوادث وإدارة المشاكل وما إلى ذلك. الهدف هو وضع ضوابط لتحقيق أعلى مستوى من جودة خدمات تقنية المعلومات مع الحد الأدنى من المخاطر التشغيلية.

١٠,١. إدارة التغيير (Change Management)

١٠,١,١ يجب التحكم في التغييرات التي تطرأ على مرافق ونظم معالجة المعلومات .
١٠,١,٢ يجب على المؤسسة إعداد وثيقة متطلبات العمل (BRD) التي ستغطي متطلبات تغييرات النظام وتأثير ذلك على العمليات والاعمال ومصفوفة الأمن وإعداد التقارير والواجهات البينية وما إلى ذلك .
١٠,١,٣ يجب أن تخضع جميع التغييرات في تطبيق الأعمال المنفذة في بيئة الإنتاج لعملية رسمية موثقة مع تفاصيل التغيير اللازمة .
١٠,١,٤ يجب الاحتفاظ بسجلات التدقيق لتطبيقات الأعمال .
١٠,١,٥ يجب أن تقوم المؤسسة بإعداد خطة اسستعادة للاحداث غير المتوقعة .
١٠,١,٦ يجب إجراء اختبار قبول المستخدم (UAT) للتغييرات والتحديثات في التطبيق قبل تنفيذها .
١٠,١,٧ يمكن إجراء اختبار التحقق من المستخدم (UVT) لما بعد التنفيذ.

١١. الخدمات المالية عبر الهاتف المحمول (Mobile Financial Services)

إن الضوابط على المعاملات عبر الهاتف المحمول مطلوبة لإدارة مخاطر العمل في بيئة غير محمية. تقوم المؤسسة بصياغة الضوابط الأمنية وتوافر النظام وقدرات الاسترداد، والتي تتناسب مع مستوى التعرض للمخاطر
١١,١ يجب اتباع المعايير الأمنية بما يتناسب مع مدى تعقيد الخدمات المقدمة.
١١,٢ يجب على المؤسسات أن تحدد بوضوح المخاطر المرتبطة بأنواع الخدمات المقدمة في عملية إدارة المخاطر.
١١,٣ يجب تنفيذ التدابير المناسبة لتخفيف وتقليل المخاطر مثل حد التعاملات، والحد من تكرار التعاملات، وفحوصات الاحتيال، وفحوصات مكافحة غسل الأموال، وما إلى ذلك اعتمادًا على فهم المخاطر، ما لم تنص الهيئة التنظيمية على خلاف ذلك.
١١,٤ يجب أن تتوافق الخدمات التي تقدمها المؤسسات عبر الهاتف المحمول مع المبادئ والممارسات الأمنية لمصادقة المعاملات.
١١,٥ يجب على المؤسسة إجراء تحليل دوري لإدارة المخاطر وتقييم أمني لعمليات الخدمات المالية عبر الهاتف المحمول واتخاذ التدابير المناسبة وفقًا لذلك.
١١,٦ يجب على المؤسسة ان تتطابق مع متطلبات "الامتثال التنظيمي" للدولة.
١١,٧ يجب الحفاظ على التوثيق الصحيح للممارسات الأمنية والمبادئ التوجيهية والأساليب والإجراءات المستخدمة في هذه الخدمات المالية عبر الهاتف المحمول وتحديثه.

١٢. أمن قاعدة البيانات (Database Security)

١٢,١. بيانات عامة (General Statements)

١٢,١,١ يجب تحديد وتوثيق نظام إدارة قواعد البيانات (DBMS) في المؤسسة وتوفير بيئة مناسبة للحماية من المخاطر التشغيلية والبيئية .

١٢,١,٢ يجب تطوير معايير الأمني التقني لنظام إدارة قواعد البيانات في المؤسسة وتطبيقها من قبل مديري إدارة قواعد البيانات.

١٢,١,٣ يجب أن يقتصر الوصول المباشر إلى قاعدة البيانات على مديري إدارة قواعد البيانات فقط؛ ويجب على المستخدمين الآخرين الوصول إلى قاعدة البيانات من خلال التطبيقات فقط .

١٢,١,٤ يجب منح الوصول إلى قاعدة البيانات وفقًا لسياسة إدارة الهوية والوصول .

١٢,١,٥ يحظر ترحيل قاعدة بيانات الأنظمة الحرجة أو نقلها من بيئة الإنتاج إلى أي بيئة أخرى.

١٢,٢. متطلبات أمن استضافة نظم إدارة قواعد البيانات (DBMS Hosting Security Requirements)

١٢,٢,١ نظام إدارة قواعد البيانات المستضافة المرتبط بمتطلبات استمرارية الأعمال والتعافي من الكوارث يجب ان يكون محدد بوضوح في العقود المبرمة مع مقدم خدمة الاستضافة، والتي تتضمن الأدوار والمسؤوليات المتبادلة من حيث النسخ الاحتياطية والاستجابة للحوادث وخطة الاستعادة وما إلى ذلك .

١٢,٢,٢ يجب أن تكون قواعد بيانات المؤسسة مفصولة منطقيًا عن قواعد البيانات المستضافة الأخرى .

١٢,٢,٣ يجب أن يكون وصول مدراء الانظمة إلى نظام إدارة قواعد البيانات مؤمنًا ومشفّرًا باستخدام آلية قوية مثل SSH أو VPN أو SSL/TLS وفقًا لسياسة التشفير الخاصة بالمؤسسة.

١٢,٣.متطلبات إدارة التغيير في نظام إدارة قواعد البيانات (DBMS Change Management Requirements)

١٢,٣,١ يجب أن تتبع التغييرات في نظام إدارة قواعد البيانات (مثل ترحيل قاعدة البيانات ونقلها إلى بيئة الإنتاج) عملية إدارة التغييرات الخاصة بالمؤسسة .

١٢,٣,٢ يجب أن يتم تحديث نظام إدارة قواعد البيانات وفقًا لسياسة إدارة التحديثات الخاصة بالمؤسسة.

١٢,٣,٣ يجب استخدام نظام إدارة قواعد البيانات المرخص والمصرح به .

١٢,٣,٤ يجب تنفيذ خطة وإجراءات التعافي من الكوارث في نظام إدارة قواعد البيانات .

١٢,٣,٥ يجب أن تحافظ المؤسسة على اتفاقية /اتفاقيات مستوى الخدمة مع البائع / البائعين لنظام إدارة قواعد البيانات في بيئة الانتاج .

١٢,٣,٦ يجب أن تكون قواعد البيانات المخزنة مشفرة وفقًا لسياسات التشفير والتصنيف الخاصة بالمؤسسة.

١٢,٤. مراقبة سجلات أحداث نظام إدارة قواعد البيانات (DBMS Event Logs Monitoring)

١٢,٤,١ يجب تفعيل سجلات أحداث نظام إدارة قواعد البيانات والاحتفاظ بها وفقًا لسياسة إدارة سجلات أحداث الأمن السيبراني ومراقبة سجلات الأحداث الخاصة بالمؤسسة.

١٢,٤,٢ يجب أن تراقب المؤسسة سجلات أحداث قاعدة بيانات الانظمة الحرجة وسلوك المستخدمين .

١٢,٤,٣ يجب مراقبة ومراجعة سجلات أحداث وسلوك مديري قاعدة بيانات النظم الحرجة بانتظام من قبل المؤسسة .

١٢,٥. المتطلبات التشغيلية (Operational Requirements)

١٢,٥,١ يجب توفير المتطلبات التشغيلية المناسبة لقاعدة البيانات مثل البيئة الآمنة وتقييد الوصول المادي إلى الأنظمة على الموظفين المصرح لهم فقط .

١٢,٥,٢ يجب مراقبة المكونات التشغيلية لقواعد البيانات من قبل تقنية المعلومات وضمان فعالية الأداء والتوافرية وسعة التخزين وما إلى ذلك.

١٢,٦. متطلبات أخرى

١٢,٦,١ يجب استخدام مؤشرات الأداء الرئيسية (KPIs) لضمان التحسين المستمر لأمن نظام إدارة قواعد البيانات .

١٢,٦,٢ يجب مراجعة متطلبات الأمن السيبراني لنظام إدارة قواعد البيانات مرة واحدة في السنة كحد أدنى، أو عند حدوث تغييرات في المتطلبات القانونية والتنظيمية ذات الصلة.

١٣. أمن الطرف الخارجي (Third party security)

١٣,١. نظرة عامة (General Statement)

١٣,١,١ يجب توثيق إجراءات موحدة ومعتمدة لإدارة علاقات المؤسسة مع الطرف الخارجي قبل وأثناء وبعد انتهاء العلاقة التعاقدية .

١٣,١,٢ يجب اختيار مقدمي خدمات الطرف الخارجي بعناية بناءً على سياسات المؤسسة والإجراءات التنظيمية والمتطلبات القانونية والتنظيمية ذات الصلة .

١٣,١,٣ يجب إجراء تقييم لمخاطر الطرف الخارجي والخدمات المقدمة لضمان سلامتها. ويتم ذلك من خلال مراجعة مشاريع الطرف الخارجي داخل المؤسسة والمراجعة الدورية لسجلات الأحداث الامنية والسيبرانية لخدمات الطرف الخارجي (إن وجدت) قبل وأثناء العلاقة التعاقدية.

١٣,١,٤ يجب أن تضمن العقود والاتفاقيات المبرمة مع طرف خارجي التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للمؤسسة والمتطلبات القانونية والتنظيمية ذات الصلة .

١٣,١,٥ يجب مراجعة العقود والاتفاقيات المبرمة مع طرف خارجي من قبل المؤسسة للتأكد من أن البنود ملزمة أثناء الاتفاقيات وأن الطرف الخارجي سيكون مسؤولاً قانونياً عن أي انتهاكات .

١٣,١,٦ يجب أن تتضمن العقود والاتفاقيات بنود عدم الإفصاح والحذف الآمن لمعلومات المؤسسة من قبل الاطراف الخارجية عند انتهاء الخدمة .

١٣,١,٧ يجب مراجعة متطلبات الأمن السيبراني للطرف الخارجي بشكل دوري .

١٣,١,٨ يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنويًا، ويجب توثيق التغييرات والموافقة عليها .

١٣,٢. متطلبات الأمن السيبراني للاستعانة بمصادر خارجية لتقنية المعلومات والخدمات المدارة من طرف خارجي

١٣,٢,١ بالنسبة للاستعانة بمصادر خارجية لتقنية المعلومات والخدمات المدارة من قبل الاطراف الخارجية، يجب اختيار الطرف الخارجي بعناية بعد التحقق مما يلي:

١٣,٢,١,١ يجب إجراء تقييم لمخاطر الأمن السيبراني وأنشطة الرقابة قبل توقيع العقود والاتفاقيات مع الأطراف الخارجية أو على التغييرات ذات الصلة في المتطلبات والقوانين واللوائح .

١٣,٢,١,٢ يجب ان يكون تقديم خدمات الاستعانة بمصادر خارجية لأصول المعلومات والتقنيات الحيوية متوافقاً مع المتطلبات القانونية والتنظيمية ذات الصلة .

١٣,٢,٢ متطلبات الأمن السيبراني لموظفي الطرف الخارجي (Third-Party Personnel Cybersecurity Requirements)

١٣,٢,٢,١ يجب إجراء تدقيق و فحص للشركات الخارجية وموظفي الخدمات الخارجية والخدمات المدارة والعاملين على الأنظمة الحرجة.

١٣,٢,٢,٢ يجب تضمين مسؤوليات الأمن السيبراني وبنود عدم الإفصاح في عقود موظفي الطرف الخارجي ويجب أن تكون سارية المفعول أثناء وبعد انتهاء علاقة العمل مع المؤسسة.

١٣,٢,٣ ضوابط المصادقة والوصول (Authentication and Access Controls)

١٣,٢,٣,١ يجب على الأطراف الخارجية تطوير واتباع عملية رسمية وموثقة بشكل جيد لمنح وإلغاء الوصول إلى جميع المعلومات والانظمة التقنية التي تعالج أو تنقل أو تخزن معلومات المؤسسة بما يتوافق مع متطلبات الأمن السيبراني للمؤسسة وأهداف ضوابط الأمن السيبراني .

١٣,٢,٣,٢ يجب توفير الوصول إلى معلومات المؤسسة ومعالجتها بطريقة آمنة ومحكومة .

١٣,٢,٣,٣ يجب تطبيق ضوابط كلمة السر لجميع المستخدمين الذين لديهم إمكانية الوصول إلى معلومات المؤسسة بما يتوافق مع متطلبات الأمن السيبراني للمؤسسة وأهداف ضوابط الأمن السيبراني .

١٣,٢,٣,٤ يجب تطبيق المصادقة متعددة العوامل (MFA) على الوصول إلى الأنظمة الحيوية التي تعالج أو تنقل أو تخزن معلومات المؤسسة.

١٣,٢,٣,٥ يجب إلغاء حقوق الوصول عند انتهاء الخدمة/إنهاء خدمة أي موظف للاطراف الخارجية لديه حق الوصول إلى معلومات المؤسسة أو أصول المعلومات والتقنيات أو في حالة حدوث تغيير في دوره الوظيفي الذي يلغي شرط استمرار الوصول .

١٣,٢,٣,٦ يجب مراجعة حقوق الوصول بانتظام من قبل الطرف الخارجي وفقًا لسياسات الأمن السيبراني للمؤسسة .

١٣,٢,٣,٧ يجب تخزين جميع سجلات التدقيق والاحتفاظ بها وإتاحتها عند طلب المؤسسة.

١٤. أمن التطبيقات (Application security)

١٤,١. تصميم ومعمارية تطبيقات الويب (Web Application Design and Architecture)

١٤,١,١ يجب أن تكون تطبيقات الويب المهمة التي سيتم تنفيذها سواء تم تطويرها داخليًا أو تم شراؤها وتتبع مبدأ المعمارية متعددة المستويات (مكونات البرنامج) ونهج التصميم متعدد الطبقات مع ٣ طبقات على الأقل، على سبيل المثال، طبقة واجهة المستخدم، وطبقة الأعمال والمكتب الخلفي أو طبقة قاعدة البيانات .

١٤,١,٢ يجب أن تستخدم تطبيقات الويب بروتوكولات الاتصال الآمنة فقط (مثل HTTPS و SFTP و TLSوغيرها).

١٤,١,٣ يجب حماية تطبيقات الويب الخارجية بواسطة جدار حماية تطبيقات الويب (WAF) من الهجمات الخارجية .

١٤,١,٤ يجب تنفيذ المصادقة متعددة العوامل لجميع تطبيقات الويب التي يستخدمها الموظفون أو الزبائن والتي يمكن الوصول إليها عبر الإنترنت .

١٤,١,٥ يجب أن تقوم تطبيقات الويب التي تنقل أو تعالج أو تخزن المعلومات المحمية بذلك بطريقة آمنة باستخدام أدوات وبروتوكولات التشفير المعتمدة (مثل SFTP وFTPS و AS2 وغيرها).

١٤,١,٦ يجب توفير بيئات آمنة لأنشطة التطوير والاختبار لضمان الفصل والعزل عن بيئة الإنتاج.

١٤,١,٧ يجب أن تستخدم تطبيقات الويب منافذ وخدمات قياسية (standard ports and services).

١٤,١,٨ يجب أن تتوافق تطبيقات الويب التي تم شراؤها من البائعين الخارجيين للمؤسسة بمتطلبات المؤسسة وسياسات الأمن السيبراني .
١٤,١,٩ يجب على المطورين استخدام الضوابط الأمنية المناسبة، مثل مصادقة نظام التشغيل، وبرامج البائعين المعتمدة، وعمليات التشفير بما يتوافق مع معيار التشفير الخاص بالمؤسسة .
١٤,١,١٠ يوصى بالاخذ بنظر الاعتبار لتطبيقات الويب المهمة ضوابط الأمن السيبراني وتقنيات الوقاية المتعلقة ب (Open Web Applications Security Project (OWASP) top 10 application security risks).

١٤,٢. الوصول المقيد والفصل بين المهام (Restricted Access and Segregation of Duties)

١٤,٢,١ يجب تحديد ضوابط إدارة الجلسات بما في ذلك توثيق الجلسات وإغلاق الجلسات ومهلة الجلسات وتطبيقها على جميع تطبيقات الويب .
١٤,٢,٢ يجب أن يكون الوصول إلى أنظمة بيئة الإنتاج محدودًا ومراقبًا وفقًا للمسؤوليات الوظيفية في المؤسسة .
١٤,٢,٣ إذا كانت المعلومات المهمة المحمية ضرورية في البيئات غير الإنتاجية ووفقًا لحاجة العمل، يجب إلغاء عناصر البيانات المحمية أو إخفاؤها أو حذفها بعد استخدامها .
١٤,٢,٤ يجب أن يقتصر مقدار المعلومات المهمة المحمية المستخدمة في بيئة غير بيئة الإنتاج على ما هو مطلوب لإجراء الاختبار .
١٤,٢,٥ يجب تقييد الوصول إلى المعلومات المحمية في البيئات غير الإنتاجية.
١٤,٢,٦ يجب ألا يُسمح للمطورين بتعديل الكود المصدري/مصدر التعليمات البرمجية والبيانات في بيئة الانتاج (production source code or production data).
١٤,٢,٧ يجب تقييد المطورين من تعديل إعدادات النظام، ما لم تتم الموافقة على ذلك .
١٤,٢,٨ في حالة استخدام حسابات الاختبار في البيئات غير الإنتاجية، يجب إزالتها قبل نقل التطبيق إلى بيئة الإنتاج .
١٤,٢,٩ يجب عدم السماح باستخدام حسابات الاختبار وبيانات الاختبار في بيئة الإنتاج .
١٤,٢,١٠ يجب تحذير مستخدمي تطبيقات الويب وتعريفهم بسياسة الاستخدام الآمن.

١٤,٣. متطلبات إدارة المخاطر (Risk Management Requirements)

١٤,٣,١ يجب إجراء تقييمات للمخاطر لتطبيقات الويب قيد التطوير أو التي تم شراؤها لتحديد الضوابط المطلوبة لتقليل مخاطر التطبيق لحدود مقبولة .
١٤,٣,٢ يجب أن تخضع جميع جهود تطوير البرمجيات التي تتم بالاستعانة بمصادر خارجية لنفس متطلبات تقييم المخاطر التي يخضع لها التطوير الداخلي .
١٤,٣,٣يجب أن تتبع تطبيقات الويب المعتمدة على لغات الماكرو أو لغات البرمجة النصية أو أدوات الطرف الخارجي (macro languages, scripting languages, or third-party tools) عمليات إدارة التغيير المعتمدة قبل التثبيت على أنظمة بيئة الإنتاج.

١٤,٤. اختبار تطبيقات الويب (Web Application Testing)

١٤,٤,١ يجب اختبار ضوابط الأمن السيبراني للتأكد من توافقها مع متطلبات الأمن السيبراني قبل إطلاقها في بيئة الإنتاج .
١٤,٤,٢ يجب اختبار الميزات الأمنية للتطبيقات الجديدة أو التغييرات المهمة على تطبيقات الويب الحالية وتوثيقها ومراجعتها بشكل صحيح قبل ترقيتها إلى بيئة الإنتاج .

١٤,٤,٣ يجب مراجعة ميزات أمن تطبيقات الويب ونتائج اختبارات التحقق من الأمن ومعالجتها مع مالكي تطبيقات الويب قبل تثبيت تطبيقات الويب .
١٤,٤,٤ يجب توثيق أدلة اختبارات التحقق الأمني وتصنيفها وفقًا لسياسة تصنيف البيانات الخاصة بالمؤسسة.
١٤,٤,٥ يجب أن تتضمن الأدلة من أجرى الاختبار، وطبيعة الاختبارات التي تم إجراؤها، ونتائج تلك الاختبارات، وأي أنشطة إصلاح مطلوبة/منفذة .
١٤,٤,٦ يجب حماية بيانات اختبار تطبيقات الويب بشكل كافٍ لضمان عدم الوصول غير المصرح به إلى المعلومات المحمية .
١٤,٤,٧ يجب اختبار تطبيقات الويب للتأكد من أن ضوابط الفصل بين الواجبات تعمل بشكل مناسب .
١٤,٤,٨ يجب اختبار تطبيقات الويب لغرض البحث عن نقاط الضعف اوالتحديثات قبل تنفيذها في بيئة الإنتاج .
١٤,٤,٩ يجب إجراء عمليات فحص الثغرات ومعالجة الثغرات التي تم تحديدها قبل تنفيذ تطبيق الويب في بيئة الإنتاج .
١٤,٤,١٠ يجب عمل فحص الثغرات لتطبيقات الويب الجديدة التي خضعت لتحديث رئيسي.
١٤,٤,١١ يجب أن تخضع تطبيقات الويب بشكل دوري لاختبار اختراق مستقل .
١٤,٤,١٢ يجب مراجعة الضوابط الأمنية لتطبيقات الويب الجديدة المطورة داخليًا والموافقة عليها قبل تنفيذ التطبيق في بيئة الإنتاج .
١٤,٤,١٣ يجب إعادة تقييم تطبيقات الويب الحالية وإعادة الموافقة عليها بعد إجراء تغيير رئيسي على التطبيق أو بعد فترة محددة مسبقًا .
١٤,٤,١٤ يجب معالجة جميع القضايا الأمنية في تطبيقات الويب التي يتم اكتشافها أثناء المراجعة الامنية للكود المصدري قبل تنفيذها في بيئة الإنتاج.

١٤,٥. الصيانة (Maintenance)

١٤,٥,١ يجب تثبيت جميع التحديثات اللازمة على تطبيق الويب في الوقت المناسب وفقًا لسياسة إدارة التحديثات الخاصة بالمؤسسة.
١٤,٥,٢ يجب استخدام نظام ترقيم التحكم في الإصدار لبيان وقت تثبيت الإصدارات المحدّثة من البرنامج .
١٤,٥,٣ يجب أن تتبع جميع طلبات التوقف عن العمل عملية إدارة التغيير .
١٤,٥,٤ يجب أن تخضع تطبيقات الويب لمراجعة الكود المصدري والمراجعة الأمنية بعد إجراء تغييرات رئيسية في الإصدار أو بعد فترة محددة مسبقًا .
١٤,٥,٥ يجب أن تخضع التغييرات على عوامل التهيئة داخل تطبيق الويب للاختبار إن أمكن .
١٤,٥,٦ يجب التحكم في عمليات التثبيت الخاصة ببيئة الإنتاج بشكل صحيح لتقليل مخاطر تعطل بيئة الإنتاج.

١٤,٦.التخلص (Disposal)

١٤,٦,١ في نهاية العمر الافتراضي لتطبيق الويب، يتم ايقاف جميع المعدات المستخدمة لاستضافة التطبيق أو لتطوير التطبيق وصيانته وفقًا لسياسة إدارة الأصول الخاصة بالمؤسسة .
١٤,٦,٢ يجب إتلاف جميع البيانات المستخدمة أو المحفوظة بواسطة تطبيقات الويب التي انتهى عمرها الافتراضي أو الاحتفاظ بها بطريقة آمنة، على النحو الذي تحدده سياسة إدارة الأصول الخاصة بالمؤسسة.
١٤,٦,٣ بالنسبة لتطبيقات الويب التي انتهى عمرها الافتراضي، يجب أرشفة الكود المصدري بحيث يمكن استرجاعها في حالة الحاجة إليها.

١٤,٧. المراقبة والتحسين (Monitoring and improvement)

١٤,٧,١ يجب مراجعة متطلبات الأمن السيبراني لتطبيقات الويب بشكل دوري.

الكشف (Detect)

خلال مرحلة الكشف يجب على المؤسسات تطوير وتنفيذ الأنشطة المناسبة لتحديد وقوع احداث الأمن السيبراني

١. المراقبة الأمنية (Security Monitoring)

١,١ يجب على المؤسسة إنشاء أنظمة وعمليات مراقبة أمنية مناسبة، لتسهيل الكشف الفوري عن الأنشطة غير المصرح بها أو الضارة من قبل الأطراف الداخلية والخارجية .

١,٢ يجب على المؤسسة تنفيذ إجراءات مراقبة الشبكة والمراقبة الأمنية باستخدام أجهزة أمن الشبكة، مثل أنظمة كشف ومنع التدخل لحماية المؤسسة من هجمات التطفل على الشبكة وكذلك توفير تنبيهات عند حدوث التدخل/ التطفل .

١,٣ يمكن للمؤسسة تطبيق أدوات المراقبة الأمنية التي تتمكن من الكشف عن التغييرات التي تطرأ على موارد تقنية المعلومات الهامة مثل قواعد البيانات أو ملفات النظام أو البيانات والبرامج، لتسهيل تحديد التغييرات غير المصرح بها .

١,٤ يجب على المؤسسة مراجعة السجلات الأمنية للأنظمة والتطبيقات وأجهزة الشبكة بانتظام للكشف عن أي حالات شاذة. يجب حماية السجلات والاحتفاظ بها لفترة محددة لتسهيل التحقيق في المستقبل .

١,٥ يجب على المؤسسة بناء قدرات للمراقبة المستمرة في الوقت الحقيقي أو شبه الحقيقي، للكشف عن الأنشطة أو الحوادث غير المعروفة وغير الطبيعية، ومن الممارسات التي تساهم في تحقيق ذلك إنشاء ما يشار إليه عمومًا باسم مركز العمليات الأمنية (SOC) ، ويجب اختبار هذه القدرات وصيانتها باستمرار.

٢. عمليات التدقيق (Audits)

عمليات التدقيق والامتثال: يجب أن تساعد جميع الجهات ذات الصلة مجلس الإدارة والإدارة العليا في تقييم وقياس كفاءة وفعالية إطار عمل المرونة السيبرانية للمؤسسة ، ويجب تقييم وقياس مدى امتثال وكفاية وكفاءة إطار عمل المرونة السيبرانية بانتظام من خلال الاختبارات اللازمة وبرامج الامتثال المستقلة وعمليات التدقيق من قبل جهات مؤهلة.

٢,١. التدقيق الداخلي (Internal Audits)

يجب على المؤسسة إجراء تدقيق داخلي

٢,١,١ يجب إجراء التدقيق الداخلي لنظام المعلومات من قبل إدارة التدقيق الداخلي للمؤسسة .

٢,١,٢ يقوم بالتدقيق الداخلي لنظم المعلومات موظفون يتمتعون بخبرة ومهارات كافية في مجال التدقيق الداخلي لنظم المعلومات .

٢,١,٣ يتم وضع خطة تدقيق سنوية لتدقيق النظام تغطي الخدمات/العمليات الاساسية/الرئيسية القائمة على التقنيات والبنية التحتية لتقنية المعلومات بما في ذلك الفروع التشغيلية .

٢,١,٤ يجب إجراء التدقيق الداخلي لنظام المعلومات بشكل دوري مرة واحدة على الأقل في السنة. ويجب الاحتفاظ بالتقرير للجهات التنظيمية عند الحاجة. كما يجب على المؤسسة التأكد من تتبع قضايا التدقيق بشكل صحيح وتسجيلها بشكل كامل ومتابعتها بشكل كافٍ وتصحيحها بشكل مرضٍ .

٢,١,٥ يجب على المؤسسة اتخاذ التدابير المناسبة لمعالجة التوصيات الواردة في تقرير التدقيق (الخارجي/الداخلي).

٢,٢. التدقيق المستقل (Independent Audit)

يجب أن تخضع حالة الأمن السيبراني لأصول المعلومات الخاصة بالمؤسسة لعمليات تدقيق شاملة ومستقلة ومنتظمة لأمن المعلومات.

٢,٣. الامتثال التنظيمي (Regulatory Compliance)

يجب وضع عملية لضمان الامتثال للمتطلبات التنظيمية ذات الصلة التي تؤثر على الأمن السيبراني في المؤسسة. ينبغي لعملية ضمان الامتثال أن:

٢,٣,١ إجراءها بشكل دوري أو عندما تصبح المتطلبات التنظيمية الجديدة سارية المفعول.

٢,٣,٢ إشراك ممثلين من المجالات الرئيسية في المؤسسة.

٢,٣,٣ تؤدي إلى تحديث سياسة ومعايير وإجراءات الأمن السيبراني لاستيعاب أي تغييرات ضرورية (إن وجدت).

٢,٤. الامتثال لمعايير القطاع الدولية (Compliance with International Industry Standards)

يجب أن تمتثل المؤسسة للوائح وتعليمات البنك المركزي العراقي والتي تشمل على سبيل المثال لا الحصر ما يلي:

٢,٤,١ معيار أمن بيانات صناعة بطاقات الدفع (PCI-DSS)

٢,٤,٢ المعيار EMV (MasterCard , Visa, Europay, technical standard)

٢,٤,٣ معيار أمن المستخدم لنظام سويفت (SWIFT/CSP) .

الاستجابة (Respond)

١. إدارة الحوادث (Incident Management)

يقع الحدث عندما يكون هناك تعطل غير متوقع في تقديم خدمات تقنية المعلومات المعتادة. ويتعين على المؤسسة إدارة مثل هذه الحوادث بشكل مناسب لتجنب سوء التعامل مع مثل هذه الحوادث التي تؤدي إلى تعطل خدمات تقنية المعلومات لفترة طويلة .

١,١ يجب على المؤسسة وضع إطار عمل لإدارة الحوادث بهدف استعادة خدمات تقنية المعلومات العادية في أسرع وقت ممكن بعد وقوع الحادث بأقل تأثير ممكن على العمليات والاعمال. يجب على المؤسسة أيضًا تحديد أدوار ومسؤوليات الموظفين المشاركين في عملية إدارة الحوادث، والتي تشمل تسجيل الحوادث وتحليلها ومعالجتها ومراقبتها .

١,٢ من المهم أن يتم منح الحوادث مستوى الخطورة المناسب. كجزء من تحليل الحوادث، يجوز للمؤسسة تفويض وظيفة تحديد وتعيين مستويات خطورة الحوادث إلى الدعم والاسناد الفني. يجب على المؤسسة تدريب موظفي الدعم والاسناد الفني على تحديد الحوادث ذات مستوى الخطورة العالية. بالإضافة إلى ذلك، يجب وضع وتوثيق المعايير المستخدمة لتقييم مستويات خطورة الحوادث .

١,٣ يجب على المؤسسة وضع إجراءات التصعيد والحل المناسبة حيث يكون الإطار الزمني للحل متناسبًا مع مستوى خطورة الحادث .
١,٤ يجب اختبار خطة التصعيد والاستجابة المحددة مسبقًا للحوادث الأمنية دورياً.
١,٥ تقوم المؤسسة بتشكيل فريق استجابة لطوارئ تقنية المعلومات يضم موظفين داخل المؤسسة يتمتعون بالمهارات الفنية والتشغيلية اللازمة للتعامل مع الحوادث .
١,٦ في بعض الحالات، قد تتطور الحوادث الكبرى بشكل سلبي إلى أزمات. يجب إبقاء الإدارة العليا على علم بتطور هذه الحوادث حتى يتسنى اتخاذ قرار تفعيل خطة التعافي من الكوارث في الوقت المناسب. يجب على المؤسسة إبلاغ البنك المركزي العراقي في أقرب وقت ممكن في حال وقوع أي كارثة .
١,٧ يجب على المؤسسة إبقاء الزبائن على علم بأي حادث كبير. إن القدرة على الحفاظ على ثقة الزبائن خلال أي أزمة أو حالة طوارئ لها أهمية كبيرة بالنسبة لسمعة المؤسسة وسلامة أعمالها.
١,٨ بما أن الحوادث قد تنجم عن العديد من العوامل، يجب على المؤسسة إجراء تحليل للأسباب الجذرية والأثر للحوادث التي تؤدي إلى تعطيل خدمات تقنية المعلومات. يجب على المؤسسة اتخاذ الإجراءات العلاجية لمنع تكرار حوادث مماثلة.
١,٩ يجب أن يغطي تقرير تحليل الأسباب الجذرية والأثر المجالات التالية :
أ) تحليل الأسباب الجذرية
- متى حدث ذلك؟
- أين حدث؟
- لماذا وكيف وقع الحادث؟
- كم مرة وقع حادث مماثل؟
- ما هي الدروس المستفادة من هذا الحادث؟
ب) تحليل الأثر
- نطاق الحادث بما في ذلك معلومات عن الأنظمة والموارد والعملاء الذين تأثروا بالحادث .
- حجم الحادث. بما في ذلك الإيرادات الضائعة والخسائر والتكاليف والاستثمارات وعدد الزبائن المتأثرين والتداعيات والعواقب على السمعة والثقة .
- خرق المتطلبات والشروط التنظيمية بسبب الحادث .
ج) التدابير التصحيحية والوقائية
- اتخاذ إجراءات تصحيحية فورية لمعالجة عواقب الحادث. يجب إعطاء الأولوية لمعالجة مخاوف الزبائن.
- تدابير لمعالجة السبب الجذري للحادث .
- تدابير لمنع وقوع حوادث مماثلة أو ذات صلة .
- يجب على المؤسسة معالجة جميع الحوادث بشكل كافٍ ضمن الأطر الزمنية المناسبة للحل ومراقبة جميع الحوادث حتى حلها.
- أثناء الاستجابة والتعافي، يجب على المؤسسة تطوير وتنفيذ الأنشطة المناسبة للتصرف فيما يتعلق بحادث الأمن السيبراني المكتشف.

٢. إدارة استمرارية الأعمال والتعافي من الكوارث

إن إدارة استمرارية الأعمال والتعافي من الكوارث مطلوبة من أجل التخطيط لمرونة الأعمال في مواجهة الحوادث، والنظر في المخاطر التشغيلية للكوارث واسعة النطاق، وكوارث مركز البيانات وخطة التعافي. الهدف الأساسي من خطة استمرارية الأعمال هو تمكين المؤسسة من التعافي في حالة وقوع كارثة وإعادة تشغيل العمليات/ الاعمال بصورة طبيعية. للتعافي بأقل قدر ممكن من الخسائر المالية والخسائر المتعلقة

بالسمعة، يجب على المؤسسة أن تضمن إمكانية استئناف العمليات الحيوية للاعمال العادية في غضون إطار زمني معقول. يجب أن تغطي خطة الطوارئ خطة استئناف الأعمال وخطة التعافي من الكوارث. كما يجب أن تتناول خطة الطوارئ أيضًا عملية النسخ الاحتياطي واستعادة المعلومات والبيانات.

٢,١. خطة استمرارية الأعمال (Business Continuity Plan-BCP)

٢,١,١ يجب أن يكون لدى المؤسسة خطة معتمدة لاستمرارية الأعمال تتناول التعافي من الكوارث لمواصلة عملها .

٢,١,٢ يجب تعميم خطة استمرارية الأعمال المعتمدة على جميع أصحاب المصلحة المعنيين. ويتلقى الجميع نسخة من الخطة المعدلة كلما حدث أي تعديل أو تغيير .

٢,١,٣ يجب الاحتفاظ بالوثائق المتعلقة بخطة استمرارية الأعمال في مكان آمن خارج الموقع الرئيسي/ الموقع البديل بالإضافة إلى الموقع الرئيسي/موقع الإنتاج. ويجب الاحتفاظ بنسخة واحدة في المكتب للرجوع إليها .

٢,١,٤ يجب تنسيق خطة استمرارية الأعمال واسنادها من خلال تحليل تأثير الأعمال (BIA) وخطة التعافي من الكوارث مع الأخذ في الاعتبار متطلبات النظام والعمليات والترابطات .

٢,١,٥ يجب أن تتناول خطة استمرارية الأعمال ما يلي:

أ) خطة العمل لاستعادة العمليات والاعمال.

ب) جهات الاتصال في حالات الطوارئ وعناوين وأرقام هواتف الموظفين والبائعين والوكالات .

ج) قائمة بالعناصر مثل النسخ الاحتياطية وأجهزة الحاسوب المحمولة ووسائط التخزين المحمولة وما إلى ذلك .

د) يجب اختبار خطة استمرارية الأعمال وخطة التعافي من الكوارث ومراجعتها مرة واحدة على الأقل سنوياً لضمان فعاليتها.

٢,٢. خطة التعافي من الكوارث (Disaster Recovery Plan-DRP)

٢,٢,١ يجب أن يكون لدى المؤسسة خطة معتمدة للتعافي من الكوارث. يجب على المؤسسة عند صياغة وانشاء خطة التعافي السريع من الكوارث أن تتضمن تحليل السيناريوهات لتحديد ومعالجة أنواع مختلفة من سيناريوهات الطوارئ. يجب على المؤسسة أن تأخذ في الاعتبار سيناريوهات مثل الانقطاعات 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 .

٢,٢,٢ يجب على المؤسسة إنشاء موقع للتعافي من الكوارث (DRS) منفصل جغرافيًا عن الموقع الرئيسي لتمكين استعادة الأنظمة الحيوية واستئناف العمليات والاعمال عند حدوث عطل في الموقع الرئيسي .

٢,٢,٣ إذا لم يكن موقع التعافي من الكوارث (DRS) منفصلاً جغرافيًا بشكل صحيح، يمكن للمؤسسة إنشاء موقع ثالث في منطقة مختلفة يتم التعامل معه كموقع للتعافي من الكوارث (DRS) بعيد عن الموقع الرئيسي (Disaster Recovery Site (DRS)/Far DC). في مثل هذه الحالة، سيتم التعامل مع DRS في موقع قريب على أنه موقع التعافي من الكوارث (DRS) القريب (Near DC) ويجب تهيئته وفقًا لذلك.

٢,٢,٤ يجب أن يكون موقع التعافي من الكوارث ومركز البيانات (الموقع القريب) مجهزًا بأجهزة ومعدات اتصالات متوافقة لدعم الخدمات الحيوية لعمليات الأعمال في حالة وقوع كارثة .

٢,٢,٥ يجب الحفاظ على الأمن المادي والبيئي لأنظمة موقع التعافي من الكوارث ومركز البيانات (الموقع القريب) .

٢,٢,٦ يجب على المؤسسة تحديد أولويات استعادة النظام واستئناف الأعمال ووضع أهداف محددة لاستعادة القدرة على العمل بما في ذلك هدف وقت الاستعادة (RTO) وهدف نقطة الاستعادة (RPO) لأنظمة وتطبيقات

تقنية المعلومات. هدف وقت الاستعادة (RTO) هو المدة الزمنية، من نقطة التعطل، التي يجب استعادة النظام خلالها. وهدف نقطة الاستعادة (RPO) يشير إلى المقدار المقبول من فقدان البيانات لنظام تقنية المعلومات أثناء حدوث كارثة .

٢,٢,٧ يجب على المؤسسة أن تأخذ في الاعتبار أوجه الترابط بين الأنظمة الحرجة عند وضع خطة التعافي وإجراء اختبارات الطوارئ.

٢,٢,٨ يمكن للمؤسسة وضع استراتيجيات وتقنيات الاستعادة مثل التوافرية في الموقع ونسخ البيانات في الوقت الفعلي لتعزيز قدرة المؤسسة على الاستعادة .

٢,٢,٩ يجب الحفاظ على أمن المعلومات بشكل صحيح طوال عملية التعافي .

٢,٢,١٠ يجب 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 .

٢,٢,١١ تقوم المؤسسة باختبار كفاءة متطلبات التعافي من الكوارث والتحقق من فعاليتها وقدرة الموظفين على تنفيذ إجراءات الطوارئ والتعافي اللازمة على الاقل سنوياً.

٢,٢,١٢ يجب على المؤسسة إشراك موظفيها في تصميم وتنفيذ حالات اختبار شاملة للتحقق من أن الأنظمة المستعادة تعمل بشكل صحيح .

٢,٢,١٣ يجب أن تشتمل وثائق اختبار التعافي من الكوارث كحد أدنى على النطاق والخطة ونتائج الاختبار. ويجب إرسال تقرير الاختبار إلى الإدارة وأصحاب المصلحة الآخرين والاحتفاظ به للضرورة المستقبلية.

٣. إدارة النسخ الاحتياطي للبيانات واستعادتها (Data Backup and Restore Management)

٣,١ يجب على المؤسسة وضع سياسة للنسخ الاحتياطي واستعادة البيانات، يجب أن يكون لكل تطبيق من تطبيقات الأعمال استراتيجية نسخ احتياطي مخططة مسبقاً ومجدولة وموثقة، والتي تتضمن عمل نسخ احتياطية آنية وغير آنية ، ونقل النسخ الاحتياطية لتأمين التخزين خارج الموقع.

٣,٢ يجب إنشاء جدول النسخ الاحتياطي المخطط له مسبقاً مفصلاً لكل تطبيق عمل بما يتوافق مع تصنيف التطبيق والمعلومات التي يدعمها ويجب أن يحدد نوع النسخ الاحتياطي المطلوب (full, partial, incremental, differential) مع المراقبة في الوقت الحقيقي لكل تفاصيل جدول النسخ الاحتياطي .

٣,٣ يجب تحديد تكرار النسخ الاحتياطية للمعلومات بما يتوافق مع تصنيف المعلومات ومتطلبات خطط استمرارية الأعمال لكل تطبيق .

٣,٤ يجب أن تتضمن تفاصيل جدول النسخ الاحتياطي المخطط له مسبقاً لكل تطبيق عمل فترة الاحتفاظ بالمعلومات التي تم نسخها احتياطيًا أو أرشفتها، ويجب أن تكون فترة الاحتفاظ متسقة مع المتطلبات القانونية والتنظيمية المحلية.

٣,٥ يجب أن تكون جميع الوسائط التي تحتوي على معلومات احتياطية معنونة بمحتوى المعلومات ودورة النسخ الاحتياطي والمعرف التسلسلي للنسخ الاحتياطي وتاريخ النسخ الاحتياطي .

٣,٦ يجب الاحتفاظ بوثائق جرد النسخ الاحتياطية وسجلاتها، والتحقق منها وتوقيعها من قبل المسؤول .

٣,٧ يجب على المؤسسة تشفير البيانات الاحتياطية في ووحدات/ وسائط التخزين التي تحتوي على معلومات حساسة أو سرية قبل نقلها خارج الموقع للتخزين .

٣,٨ يجب الاحتفاظ بنسخة واحدة على الأقل من النسخ الاحتياطية في الموقع لوقت التسليم الحرج .

٣,٩ يجب توثيق عملية استعادة المعلومات من كل من التخزين الاحتياطي في الموقع وخارج الموقع .

٣,١٠ يجب أن تقوم المؤسسة بإجراء اختبار دوري والتحقق من قدرة استرجاع عمليات النسخ الاحتياطية وتقييم ما إذا كانت كافية وفعالة بما فيه الكفاية لدعم عملية استرجاع المعلومات في المؤسسة.

التوعية (Awareness)

١. برامج التوعية (Awareness Program)

ان برامج التوعية تكون ناجحة فقط إذا شعر المستخدمون بأن المحتوى يصب في مصلحتهم ويتناسب مع احتياجاتهم المصرفية. ولإعداد برنامج توعية مثمر، تحتاج المؤسسة إلى تحديد الموظفين ومواد التوعية والإعلانات والمكافآت.

١,١ يجب تحديد احتياجات الحضور المستهدف، والحصول على الميزانيات المناسبة، وتحديد الأولويات .

١,٢ يجب أن تذكر خطة العمل بوضوح الأنشطة الرئيسية مع الموارد المطلوبة والجداول الزمنية والاهداف الرئيسية .

١,٣ يجب على المؤسسة إنشاء ونشر المحتوى المناسب .

١,٤ الأهداف المشتركة لبرنامج التوعية هي:

أ) تقديم معلومات عامة ومحددة حول اتجاهات مخاطر الاحتيال أو أنواعها أو ضوابطها للأشخاص الذين يحتاجون إلى معرفتها .

ب) مساعدة الزبائن على تحديد المجالات المعرضة لمحاولات الاحتيال وتوعيتهم بمسؤولياتهم فيما يتعلق بمنع الاحتيال .

ج) تحفيز الأفراد على اعتماد المبادئ التوجيهية أو الممارسات الموصى بها .

د) خلق ثقافة أمنية أقوى مع فهم والتزام أفضل .

هـ) المساعدة في تقليل عدد الحوادث ومداها، وبالتالي تقليل التكاليف بشكل مباشر (خسائر الاحتيال) وبشكل غير مباشر (تقليل الحاجة إلى التحقيق).

١,٥ يجب على المؤسسة إيصال محتوى الرسالة الصحيحة إلى الجمهور المناسب باستخدام قنوات الاتصال الأكثر فعالية.

١,٦ يمكن إنشاء ضمانات بناء الوعي في شكل

أ) المنشورات والكتيبات

ب) خدمة الرسائل القصيرة (SMS) النصية

ج) نصائح للسلامة

د) المواد التعليمية

هـ) الإيصالات التي يتم صرفها عن طريق أجهزة الصراف الآلي/نقاط البيع

و) شاشات التوقف المؤقتة (Screensavers)

ز) النشرات الإخبارية الإلكترونية

ح) أقراص DVD تحتوي على دراسات حالة ومقاطع فيديو تفاعلية.

ط) يتم تشغيل الرسائل المسجلة أثناء فترة انتظار المكالمات الهاتفية المصرفية

١,٧ نظرًا لأن الزبائن يحصلون على المعلومات من مصادر متنوعة، يمكن استخدام أكثر من قناة اتصال واحدة لإشراكهم بنجاح .

أ) الحملات الإعلانية من خلال وسائل الإعلام المطبوعة والتلفزيونية

ب) شاشات الصراف الآلي والبريد الإلكتروني والرسائل النصية القصيرة

ج) موقع إلكتروني مشترك يتم تطويره بمحتوى من جميع أصحاب المصلحة

د) المجموعات والألعاب والملفات الشخصية على وسائل التواصل الاجتماعي
ه) الإعلانات على مواقع التسوق عبر الإنترنت
و) اللوحات الإعلانية
ز) وحدات التدريب عبر الإنترنت والعروض التوضيحية المستضافة على هذا الموقع
ح) إرشادات تفاعلية عن طريق خطوط مساعدة هاتفية
ط) لقاءات الزبائن والجلسات التفاعلية مع المتخصصين

١,٨ لا يمكن أن يحدث التحسين المستمر دون معرفة كيفية عمل البرنامج الحالي. يجب تصميم وتنفيذ استراتيجية تغذية راجعة مفحوصة جيدا.

٢. التوعية الأمنية والتدريب (Security Awareness and Training)

٢,١ نظرًا للتطور السريع للتقنيات، يجب على المؤسسة التأكد من حصول جميع الموظفين المعنيين على التدريب المناسب والتعليم والتحديثات والتوعية بأنشطة الأمن السيبراني ذات الصلة بمهامهم الوظيفية .
٢,٢ يجب على المؤسسة أيضًا ضمان الحد الأدنى من التدريب الاساسي للأعمال لموظفي تقنية المعلومات .
٢,٣ يجب على المؤسسة تنظيم تدريب/ورشة عمل للتوعية الأمنية لجميع الموظفين .
٢,٤ يجب أن تضمن المؤسسة توفير التدريب/التوعية الكافية لفريق التدقيق في نظم المعلومات مع الأخذ في الاعتبار أي خدمات مصرفية جديدة وتغييرات تقنية.

٣. تثقيف الزبائن (Customer Education)

مع ظهور الخدمات المصرفية الإلكترونية، لم تعد تجربة الزبون المصرفية تحت سيطرة المؤسسة بالكامل. في عصر نموذج الخدمة المصرفية الذاتية، يجب أن يكون الزبون أيضًا مجهزًا للقيام بالخدمات المصرفية الآمنة من خلال المساعدة الذاتية. كثيرًا ما يقال إن أفضل دفاع ضد الاحتيال هو وعي الزبون. ومع قيام المحتالين باستمرار بابتكار حيل احتيالية أكثر تنوعًا وتعقيدًا باستخدام تقنيات التكنولوجيا المتقدمة وتقنيات الهندسة الاجتماعية للوصول إلى حسابات ضحاياهم، يصبح تسريع وتيرة الوعي بين الزبائن أمرًا ضروريًا .
من المهم أيضًا توعية أصحاب المصلحة الآخرين، بما في ذلك موظفي المؤسسات المالية والمصرفية، الذين يمكنهم بعد ذلك العمل كأشخاص مرجعيين لاستفسارات الزبائن، وموظفي إنفاذ القانون للاستجابة لشكاوى الزبائن بشكل أكثر فهمًا، ووسائل الإعلام لنشر المعلومات الدقيقة وفي الوقت المناسب.

الاختبار (Testing)

١. تقييم الثغرات الأمنية واختبار الاختراق (Vulnerability Assessment and Penetration Testing)

تقييم الثغرات الأمنية (VA) هي عملية تحديد وتقييم واكتشاف الثغرات الأمنية في النظام .
١,١ يجب على المؤسسة إجراء اختبارات تقييم الثغرات الأمنية بانتظام للكشف عن الثغرات الأمنية في بيئة تقنية المعلومات .
١,٢ يجب على المؤسسة استخدام مزيج من التقنيات الاوتوماتيكية و اليدوية لإجراء تقييم شامل للثغرات الأمنية. بالنسبة للنظم القائمة على التطبيقات، يجب أن يشمل نطاق تقييم الثغرات الأمنية الثغرات الشائعة (مثل SQL injection, cross-site scripting, etc) .
١,٣ يجب على المؤسسة إنشاء عمليات لمعالجة المشكلات التي تم تحديدها في تقييم الثغرات الأمنية ومن ثم إجراء التحقق من صحة المعالجة للتحقق من معالجة الثغرات بشكل كامل .

١,٤ يجب على المؤسسة إجراء اختبارات الاختراق لإجراء تقييم متعمق للوضع الأمني للنظام من خلال محاكاة هجمات فعلية على النظام. يجب على المؤسسة إجراء اختبارات الاختراق على البنية التحتية للشبكة والأنظمة القائمة على الإنترنت بشكل دوري أو حسب الحاجة .

المراجع

1. “ISO/IEC 27001” International Information Security Standard published
2. "ISO/IEC 27005". International Organization for Standardization.
3. NIST Cybersecurity Framework