سياسات أمن المعلومات

الملخص
تم إعداد وثيقة سياسة أمن المعلومات للتعبير بوضوح عن توقعات الإدارة فيما يتعلق بتنفيذ وصيانة أمن المعلومات.

التصنيف: عام

حقوق النشر الخاصة بالدليل

المحتويات

ا. ضبط الوثائق

النسخة	التاريخ

تمت الموافقة عليها من قبل	
الإدارة المسؤولة	
الحفظ	

II. الاختصارات الرئيسية

#	الاختصار	الوصف
1	LAN	الشبكة المحلية
2	IT	تقنية المعلومات
3	HR	الموارد البشرية
4	BU	وحدة الأعمال
5	ISS	قسم أمن المعلومات

1. المقدمة

1.1 الغرض والنطاق

1.1.1 تم إعداد وثيقة سياسة أمن المعلومات لشركة التجارية للتعبير بوضوح عن توقعات الإدارة فيما يتعلق بتنفيذ وصيانة أمن المعلومات، وكذلك القواعد التي يجب اتباعها لتعزيز مستوى الشركة في مجال أمن المعلومات.

1.1.2 الغرض من هذه السياسة هو وضع التوجيهات اللازمة للحفاظ على سرية المعلومات وسلامتها وتوافرها، بالإضافة إلى جميع العمليات التجارية والأنظمة والتطبيقات الداعمة لها.

1.1.3 الهدف من هذه السياسة هو توضيح مجموعة رسمية من القواعد والتوجيهات الواجب الالتزام بها من أجل حماية أصول المعلومات الخاصة بشركة التجارية (التجارية) من التهديدات سواء كانت داخلية أو خارجية، متعمدة أو عرضية. وتتطرق هذه الوثيقة إلى أساليب الحماية الأمنية اللازمة لحفظ أصول المعلومات التابعة للشركة، بما في ذلك:

- المعلومات التي تحتفظ بها التجارية أو تعالجها نيابةً عن المستخدمين أو للأغراض الداخلية.
- المعلومات التي يحتفظ بها طرف ثالث أو يعالجها نيابةً عن التجارية (مثل المورّدين الذين يقدمون خدمات تقنية ولديهم وصول إلى أنظمة الشركة، أو المورّدين الذين يتم إسناد عمليات الأعمال إليهم).
- تقنيات المعلومات والأنظمة.
- موظفو التجارية.
- المباني والمرافق والمقار والعقارات الأخرى المملوكة أو المشغولة من قبل التجارية.
- رأس المال الفكري للشركة.
- سمعة التجارية ومصداقيتها واستمراريتها.

1.1.4 توفر وثيقة سياسة أمن المعلومات الخاصة بشركة التجارية التوجيهات اللازمة لجميع المستخدمين في المقر الرئيسي للشركة (سواء كانوا موظفين بدوام كامل أو جزئي أو متعاقدين)، وكذلك في وحدات الأعمال (BUs) والمواقع التابعة. ويجب على جميع المستخدمين الالتزام بالتعليمات الواردة في هذه السياسات لتحقيق أهداف ومتطلبات التجارية لحماية أصولها المعلوماتية. وتنطبق هذه السياسة على جميع الأنظمة المملوكة و/أو المُدارة من قبل موظفي التجارية، بالإضافة إلى الأنظمة التي يتم تشغيلها من قبل طرف ثالث لصالح الشركة

1.1.5 تُستكمل هذه السياسة بقائمة من السياسات الأمنية الأخرى التي يتم تطويرها وصيانتها من قبل قسم أمن المعلومات لمعالجة المتطلبات الأمنية في مختلف مجالات أمن المعلومات. وقد يتم دعم هذه السياسات بعدد من المعايير والعمليات والإجراءات والإرشادات التي تحددها الإدارات المختلفة بهدف تلبية متطلبات السياسة، وتوفير التوجيهات اللازمة للمستخدمين للالتزام بها في عملياتهم اليومية.

1.2 الالتزام بسياسة أمن المعلومات

1.2.1 لا يمكن تحقيق التنفيذ الناجح لسياسات أمن المعلومات في التجارية من دون تعاون جميع المستخدمين في الشركة. ومن الضروري للحفاظ على ثقافة أمن المعلومات أن يكون جميع المستخدمين على دراية كاملة بالمتطلبات الأمنية المحددة في وثيقة سياسة أمن المعلومات لدى التجارية، وأن يلتزموا بها التزامًا تامًا في جميع الأوقات.

1.2.2 سيتم نشر هذه السياسة وتوزيعها داخل شركة التجارية بحيث يتمكن الموظفون من قراءتها وفهم السياسات المطبقة عليهم.

1.2.3 يتعين على مسؤولي العمليات، ضمن نطاق صلاحياتهم، ضمان التزام جميع الموظفين والمتعاقدين والأطراف الثالثة بسياسة وإجراءات أمن المعلومات.

1.2.4 يجب على جميع المستخدمين (الموظفين، المتعاقدين، والمستشارين) فهم مسؤوليتهم والإقرار بها فيما يتعلق بالامتثال لسياسة أمن المعلومات الخاصة بشركة التجارية.

1.2.5 يجب على جميع المستخدمين الإقرار (سواء إلكترونيًا عبر البريد الإلكتروني أو شاشة الدخول، أو يدويًا من خلال توقيع عقد/نموذج رسمي) بأنهم سيلتزمون بجميع سياسات التجارية، وأن أي عدم امتثال أو إساءة استخدام لمرافق معالجة المعلومات قد يؤدي إلى خرق للامتثال.

1.2.6 يتعين على مسؤولي العمليات التأكد من أن جميع الإجراءات الأمنية ضمن نطاق مسؤولياتهم يتم تنفيذها بشكل صحيح لضمان الامتثال لسياسة وإجراءات ومعايير أمن المعلومات الخاصة بشركة التجارية.

1.3 الالتزام الفني

1.3.1 يجب أن تشمل المراجعات الفنية التحقق من الالتزام بالسياسات والإجراءات والمعايير الفنية.

1.3.2 يجب أن يتم إجراء أي مراجعة أو فحص للامتثال الفني حصراً من قبل أشخاص مختصين ومخوّلين، أو تحت إشرافهم. ويجب أن يكون هذا الشخص ذا خبرة عملية تؤهله لإجراء المراجعة باستخدام أدوات آلية، بحيث يُنتج تقريرًا فنيًا يتم تفسيره لاحقًا من قبل مختص تقني.

1.3.3 يجب تسجيل نتائج المراجعات والإجراءات التصحيحية المقابلة لها والاحتفاظ بها.

1.4 المسؤوليات

1.4.1 لجنة المخاطر والتدقيق / مجلس الإدارة

- الإشراف علي إدارة أمن المعلومات وبرامج التوعية داخل الشركة بما يضمن تعزيز وحماية سرية المعلومات وسلامتها وتوافرها
- التأكد من فعالية إدارة ومتابعة أمن المعلومات على مستوى الشركة.
- اعتماد سياسة أمن المعلومات والسياسات والأطر الداعمة ذات الصلة.

1.4.2 إدارة المخاطر / الرئيس التنفيذي للشؤون الفنية

- تعزيز الوعي الأمني من خلال التواصل الفعّال لسياسات وممارسات أمن المعلومات.
- الحفاظ على سرية وسلامة وتوافر معلومات وأنظمة وتطبيقات التجارية) التجارية (والتحكم بها.
- تقليل تعرض الشركة للمخاطر الناتجة عن فقدان أو تلف أو تعديل أو إساءة استخدام أو سرقة المعلومات.
- الالتزام بالمتطلبات القانونية والتنظيمية وإطار إدارة المخاطر الخاص بالشركة.
- ضمان الاتساق والتنسيق والتواصل بين جميع المبادرات المتعلقة بأمن المعلومات عبر وحدات الأعمال والتقنية في الشركة.
- ضمان توفير الدعم اللازم على مستوى الشركة لتنفيذ سياسات أمن المعلومات بين موظفي التجارية، بما في ذلك الموردين الخارجيين والمتعاقدين

1.4.3 قسم أمن المعلومات

- إعداد وصيانة سياسة أمن المعلومات الخاصة بشركة التجارية، والسياسات الأمنية الداعمة، والمعايير، والإرشادات.
- اعتماد جميع معايير وإرشادات أمن المعلومات.
- مراقبة الامتثال لهذه السياسة والسياسات الداعمة للتأكد من أنها تلبّي متطلبات أمن المعلومات في الشركة.
- تقديم الضمان للإدارة بأن أمن المعلومات فعّال، ويعالج المخاطر المحددة، ومتوافق مع معايير أمن المعلومات المعتمدة.
- ضمان أن الوصول إلى البنية التحتية لتقنية المعلومات – بما في ذلك الخوادم والشبكات وأنظمة التطبيقات – وكذلك أدوار المستخدمين وصلاحيات الوصول يتم وفقًا لسياسات أمن المعلومات.
- التنسيق مع وحدات الأعمال لضمان أن الصلاحيات الممنوحة للمستخدمين تكون وفق مبدأ "الحاجة إلى المعرفة" ومرتبطة بمتطلبات الأدوار الوظيفية.
- متابعة ومراجعة الممارسات والآليات للتأكد من الامتثال للسياسة المعتمدة.
- إجراء تقييمات الثغرات الأمنية على أنظمة تقنية المعلومات وتطوير استراتيجيات للتخفيف من المخاطر بالتنسيق مع إدارة المخاطر.
- التحقيق في حوادث وانتهاكات أمن المعلومات، ورفع تقارير بشأنها، واتخاذ الإجراءات المناسبة وإحالتها للإدارة العليا
- تقديم التوجيه والمشورة فيما يخص تصميم وتنفيذ متطلبات أمن المعلومات.
- تنفيذ برامج توعية مناسبة بأمن المعلومات تشمل جميع المستخدمين.

1.4.4 رئيس قسم تقنية المعلومات

- تصميم وتطوير وتطبيق التدابير الأمنية الفعّالة عبر دورة حياة كل نظام، بما يضمن توافق الأنظمة والتطبيقات مع السياسات والمعايير الأمنية المعتمدة.
- ضمان إدارة وتشغيل أنظمة تقنية المعلومات وفقًا للمعايير والإرشادات المحددة لأمن المعلومات.
- إعداد سجل لحصر أصول تقنية المعلومات الخاصة بشركة التجارية، والحفاظ عليه ومراجعته بشكل دوري.
- ضمان تطوير خطط شاملة للتعافي من كوارث تقنية المعلومات، بحيث تتضمن السيناريوهات المحتملة المرتبطة بالحوادث السيبرانية.
- الإبلاغ عن حالات عدم الامتثال لسياسة الأمن وحوادث أمن المعلومات.

1.4.5 مدير إدارة الموارد البشرية

- إدارة أمن الأفراد، بما في ذلك التدقيق على الموظفين والمتعاقدين الجدد وتزويدهم بالتعليمات اللازمة.
- إبلاغ الإدارات المعنية، بما في ذلك قسم أمن المعلومات، بحركة الموظفين أو انتقالاتهم بين مجموعات الأعمال.
- تقديم المشورة والتواصل بشأن المعلومات ذات الصلة بالحاجة إلى إلغاء صلاحيات الوصول المادي والمنطقي للموظفين والمتعاقدين الذين لم تعد لديهم حاجة إلى الوصول.
- تنظيم برامج توعية خاصة بأمن المعلومات للموظفين والمتعاقدين بالتنسيق مع قسم أمن المعلومات.
- تنفيذ الإجراءات التأديبية وفقًا لسياسة التحقيق والانضباط المعتمدة.
- تطبيق الضوابط اللازمة لتأمين المخاطر المتعلقة بالجوانب المادية والبيئية.

1.4.6 رؤساء قطاعات الأعمال

- اتخاذ الخطوات المعقولة والفعّالة من حيث التكلفة ضمن نطاق مسؤولياتهم وصلاحياتهم للحفاظ على توافر المعلومات وسلامتها وسريتها.
- فهم المخاطر الأمنية التي تؤثر على قطاع أعمالهم، وتحمل المسؤولية عن المخاطر الأمنية المرتبطة بهذا القطاع، وتطوير المتطلبات استنادًا إلى استراتيجيات التخفيف الموضوعة من قبل مسؤول أمن المعلومات لحماية المعلومات التجارية الحرجة.
- قبول المخاطر المتبقية في الحالات التي يتعذر فيها تنفيذ الضوابط الأمنية.
- إيصال سياسة أمن المعلومات والسياسات الداعمة إلى الموظفين الخاضعين لسلطتهم، وضمان التطبيق الفعّال لهذه السياسات داخل قطاعات أعمالهم.

1.4.7 موظفو شركة التجارية

- الالتزام بهذه السياسة وجميع السياسات والإجراءات الداعمة المطبقة ضمن نطاق عملهم وفي العمليات اليومية.
- ضمان عدم الكشف غير المصرّح به عن معلومات عملاء الشركة أو معلوماتها التجارية، سواء أثناء فترة العمل أو بعد انتهائها.
- استخدام البرمجيات والأنظمة المعتمدة من قبل الشركة فقط.
- الإبلاغ عن حوادث أمن المعلومات إلى المديرين المباشرين وقسم أمن المعلومات، بما في ذلك حالات عدم الامتثال من قبل الزملاء.

1.5 المراجعة والمتابعة

سيتم مراجعة هذه السياسة سنويًا كجزء من المراجعة الإدارية الشاملة لقياس فعالية إدارة أمن المعلومات في شركة التجارية. كما ستتم مراجعة السياسة استجابةً للتغيرات الجوهرية الناتجة عن الحوادث الأمنية و/أو التغييرات في البنية التنظيمية أو التقنية.

1.6 انتهاك السياسة

- يجب على جميع الأفراد قراءة هذه السياسة وفهمها والالتزام بمحتواها وبجميع السياسات الأمنية الداعمة ذات الصلة.
- أي فرد ينتهك سياسة أمن المعلومات أو أي من السياسات الأمنية الداعمة، أو يسمح عمدًا أو عن إهمال للأفراد الخاضعين لإشرافه بانتهاكها، يكون عرضةً لاتخاذ إجراءات تأديبية بحقه وفقًا لإجراءات الانضباط المعتمدة في إدارة الموارد البشرية بشركة التجارية<
- إن الكشف غير المصرح به عن معلومات عملاء التجارية سيترتب عليه اتخاذ إجراءات قانونية ضد المستخدم وفقًا للقانون الكويتي.

1.7 الاستثناءات على السياسة

يجب أن تتم مراجعة جميع الاستثناءات على هذه السياسة من قبل قسم أمن المعلومات(ISS) ، وأن تُرفع إلى إدارة المخاطر / الرئيس التنفيذي للشؤون الفنية / لجنة المخاطر والتدقيق، وذلك وفقًا لطبيعة الاستثناء الأمني. يجب أن تتم الموافقة على جميع الاستثناءات من قبل الرئيس التنفيذي للشؤون الفنية

1.8 اعتماد السياسة

يتم اعتماد سياسة أمن المعلومات من قبل مجلس إدارة شركة التجارية.

2. سياسة الاستخدام المقبول

2.1 الغرض

يتمثل الغرض من سياسة الاستخدام المقبول لشركة التجارية في وضع الممارسات المقبولة المتعلقة باستخدام موارد المعلومات الخاصة بالشركة، وذلك لحماية سرية المعلومات وسلامتها وتوافرها، سواء كانت مُنشأة أو مُجمَّعة أو مُدارة من قبل الشركة.

2.2 النطاق المستهدف

تسري سياسة الاستخدام المقبول لشركة التجارية على أي فرد أو جهة أو عملية تتعامل مع أي من موارد المعلومات التابعة لشركة التجارية.

2.3 السياسة العامة

- يتحمل الموظفون المسؤولية عن الالتزام بسياسات التجارية عند استخدام موارد المعلومات الخاصة بالشركة و/أو خلال وقت العمل في الشركة. وفي حال عدم وضوح المتطلبات أو المسؤوليات، يجب طلب المساعدة من قسم أمن المعلومات.
- التزامًا بممارساتنا الشاملة لحماية البيانات، تُطبّق هذه السياسة الخاصة بأمن المعلومات بالتوازي مع سياسة تصنيف البيانات. حيث توفر سياسة تصنيف البيانات إرشادات لتصنيف البيانات وفقًا لحساسيتها وأهميتها، مما يحدد بدوره التدابير الأمنية المناسبة الواردة في هذه السياسة. وتشكل هاتان السياستان معًا جزءًا أساسيًا من الإطار الشامل لأمن البيانات، ويجب تنفيذهما وصيانتهما باستمرار عبر جميع وظائف الشركة.
- يجب على الموظفين الإبلاغ فورًا عن أي سرقة أو فقدان أو إفصاح غير مصرّح به لمعلومات الشركة السرية أو الداخلية إلى قسم أمن المعلومات.
- يجب على الموظفين الامتناع تمامًا عن القيام بأي نشاط قد يؤدي إلى
  - مضايقة أو تهديد أو إساءة معاملة الآخرين.
  - التأثير سلبًا على أداء موارد المعلومات الخاصة بالشركة
  - حرمان موظفي الشركة المصرّح لهم من الوصول إلى موارد المعلومات.
  - الحصول على موارد إضافية بخلاف المخصصة لهم.
  - أو التحايل على ضوابط أمن الحاسوب المعتمدة في الشركة.
- يجب على الموظفين عدم تنزيل أو تثبيت أو تشغيل أي برامج أو أدوات أمنية تكشف أو تستغل نقاط الضعف في النظام. على سبيل المثال، لا يجوز لموظفي الشركة تشغيل برامج كسر كلمات المرور أو برامج تحليل الحزم أو أدوات فحص المنافذ أو أي برامج غير معتمدة أخرى على موارد المعلومات الخاصة بالشركة، ويُسمح فقط لموظفي تقنية المعلومات المخوّلين بتثبيت أي برامج، وذلك بما يتوافق مع إجراءات تثبيت البرامج المعتمدة، باستثناء مسؤولي النظام (IT Administrators).
- جميع الاختراعات وحقوق الملكية الفكرية والمعلومات المملوكة، بما في ذلك التقارير والرسومات والمخططات وأكواد البرمجيات والبرامج الحاسوبية والبيانات والمصنفات والمعلومات الفنية، التي يتم تطويرها أثناء وقت العمل في الشركة و/أو باستخدام موارد المعلومات الخاصة بها، تُعتبر ملكًا حصريًا لشركة التجارية.
- يجب إدارة استخدام التشفير بطريقة تتيح للموظفين المصرّح لهم في الشركة الوصول الفوري إلى جميع البيانات عند الحاجة.
- يتم توفير موارد المعلومات الخاصة بالشركة لدعم أعمال الشركة، ولا يجوز استخدامها لتحقيق مكاسب مالية شخصية
- يُتوقع من الموظفين التعاون الكامل مع التحقيقات الخاصة بالحوادث الأمنية.
- يُتوقع من الموظفين احترام جميع الحمايات القانونية والامتثال لها، بما في ذلك تلك المتعلقة ببراءات الاختراع وحقوق النشر والعلامات التجارية وحقوق الملكية الفكرية لأي برامج أو مواد يتم الاطلاع عليها أو استخدامها أو الحصول عليها باستخدام موارد المعلومات الخاصة بشركة التجارية.
- يجب على الموظفين عدم الوصول عمدًا إلى أو إنشاء أو تخزين أو نقل أي مواد قد تعتبرها شركة التجارية (التجارية) مسيئة أو غير لائقة أو فاحشة.

2.4 سياسة إدارة الوصول

- يتم منح صلاحية الوصول إلى المعلومات وفقًا لمبدأ "الحاجة إلى المعرفة".
- يُسمح للموظفين باستخدام عناوين الشبكة والخوادم التي تم تخصيصها لهم فقط من قبل قسم تقنية المعلومات في التجارية، ولا يجوز لهم محاولة الوصول إلى أي بيانات أو برامج موجودة على أنظمة الشركة من دون تصريح أو موافقة صريحة.
- يجب أن تتم جميع اتصالات الوصول عن بُعد إلى الشبكات والبيئات الداخلية الخاصة بالشركة عبر شبكات خاصة افتراضية معتمدة ومقدمة من الشركة.
- لا يجوز للموظفين الكشف عن أي معلومات وصول لأي شخص غير مصرح له صراحةً باستلام تلك المعلومات.
- يُحظر على الموظفين مشاركة بيانات الاعتماد الخاصة بهم في أنظمة الشركة، بما في ذلك:
  - كلمات مرور الحسابات.
  - أرقام التعريف الشخصية.
  - رموز الأمان (مثل البطاقات الذكية).
  - بطاقات الوصول و/أو المفاتيح.
  - الشهادات الرقمية.
- أي معلومات أو أجهزة مشابهة تُستخدم للتعريف والمصادقة.
- يجب الإبلاغ عن فقدان أو سرقة بطاقات الوصول أو رموز الأمان أو المفاتيح في أقرب وقت ممكن إلى الشخص المسؤول عن إدارة المرافق الخاصة بموارد المعلومات.
- قد يتم فرض رسوم خدمة على بطاقات الوصول أو رموز الأمان أو المفاتيح المفقودة أو المسروقة أو غير المُعادة.

2.5 سياسة المصادقة / كلمات المرور

- يُلزم جميع الموظفين بالحفاظ على سرية معلومات المصادقة الشخصية.
- يجب أن تقتصر مشاركة معلومات المصادقة الجماعية/المشتركة على الأعضاء المصرح لهم فقط ضمن المجموعة.
- يجب إنشاء جميع كلمات المرور، بما في ذلك كلمات المرور الأولية و/أو المؤقتة، وتنفيذها وفقًا للقواعد المعتمدة من شركة التجارية.
  - يجب أن تستوفي جميع المتطلبات المحددة في معيار المصادقة الخاص بالشركة، بما في ذلك الحد الأدنى للطول، والتعقيد، ومتطلبات تغيير/تدوير كلمات المرور.
  - يجب ألا تكون كلمة المرور سهلة الربط بصاحب الحساب باستخدام بيانات مثل: اسم المستخدم، الرقم المدني، الأسماء المستعارة، أسماء الأقارب، تاريخ الميلاد، إلخ.
  - يجب ألا تتضمن كلمات شائعة، مثل كلمات القواميس أو الاختصارات.
  - يجب ألا تكون مماثلة لكلمات المرور المستخدمة في الأغراض غير العملية (خارج نطاق العمل).
  - يجب الاحتفاظ بسجل تاريخ كلمات المرور لمنع إعادة استخدامها.
  - يجب استخدام كلمات مرور فريدة لكل نظام، كلما كان ذلك ممكنًا.
  - لا يجوز للمستخدمين الكشف عن كلمات مرور حساباتهم لأي شخص. كما لا يجوز لموظفي الدعم الفني أو المتعاقدين لدى الشركة طلب كلمات مرور الحسابات مطلقًا
- يجب إعادة رموز الأمان (مثل البطاقات الذكية) عند الطلب أو عند انتهاء العلاقة مع شركة التجارية، إن كانت قد صُرفت للمستخدم
- إذا كان هناك شك في أمان كلمة المرور، يجب تغييرها فورًا.
- يجب على الموظفين عدم التحايل على إدخال كلمات المرور باستخدام ميزات حفظ كلمات المرور في التطبيقات، أو عبر السكربتات المدمجة، أو من خلال كلمات مرور مُشفَّرة/مكتوبة بشكل ثابت داخل برمجيات العميل.

2.6 سياسة المكتب النظيف / الشاشة النظيفة

- يجب على الموظفين تسجيل الخروج من التطبيقات أو خدمات الشبكة عند عدم الحاجة إليها.
- يجب على الموظفين تسجيل الخروج أو قفل أجهزة الحاسوب المكتبية والمحمولة عند ترك أماكن عملهم دون مراقبة.
- يجب إزالة المعلومات السرية أو الداخلية أو وضعها في درج أو خزانة ملفات مقفلة عند ترك محطة العمل دون مراقبة، وكذلك في نهاية يوم العمل إذا لم يكن بالإمكان تأمين مكان العمل بوسائل أخرى.
- يجب إزالة المتعلقات الشخصية، مثل الهواتف والمحافظ والمفاتيح، أو وضعها في درج أو خزانة مقفلة عند ترك مكان العمل دون مراقبة.
- يجب أن تكون خزائن الملفات التي تحتوي على معلومات سرية مقفلة عند عدم استخدامها أو عند تركها دون مراقبة.
- يجب عدم ترك المفاتيح المادية و/أو الإلكترونية المستخدمة للوصول إلى المعلومات السرية على مكتب غير مراقب أو في مكان عمل غير مؤمّن ماديًا.
- يجب تأمين أجهزة الحاسوب المحمولة إما باستخدام كابل قفل أو وضعها في درج أو خزانة مقفلة عند ترك مكان العمل دون مراقبة أو في نهاية يوم العمل إذا لم يكن الجهاز مُشفّرًا.
- يجب عدم كتابة كلمات المرور أو لصقها على الحاسوب أو أسفله أو في أي مكان آخر يسهل الوصول إليه ماديًا.
- يجب إزالة النسخ الورقية من المستندات التي تحتوي على معلومات سرية من الطابعات وآلات الفاكس فور طباعتها.

2.7 سياسة أمن البيانات

- يجب على الموظفين استخدام وسائل اتصال مشفّرة ومعتمدة كلما تم إرسال معلومات سرية عبر شبكات الحاسوب العامة (الإنترنت).
- يجب تأمين المعلومات السرية المنقولة عبر خدمات البريد بما يتوافق مع سياسة تصنيف أصول المعلومات.
- لا يجوز استخدام إلا تطبيقات الحوسبة السحابية المعتمدة لمشاركة أو تخزين أو نقل المعلومات السرية أو الداخلية.
- يجب مشاركة المعلومات والتعامل معها ونقلها وحفظها وإتلافها بما يتناسب مع درجة حساسيتها.
- يجب على الموظفين تجنب إجراء محادثات سرية في الأماكن العامة أو عبر قنوات اتصال غير آمنة أو في المكاتب المفتوحة أو قاعات الاجتماعات.
- يجب نقل المعلومات السرية إما عن طريق موظف من شركة التجارية أو عبر ناقل معتمد من قبل إدارة تقنية المعلومات.
- يجب التخلص بشكل آمن من جميع الوسائط الإلكترونية التي تحتوي على معلومات سرية. ويرجى التواصل مع قسم تقنية المعلومات للحصول على التوجيه أو المساعدة عند الحاجة.

2.8 سياسة البريد الإلكتروني والاتصالات الإلكترونية

- يُحظر إعادة توجيه الرسائل الإلكترونية تلقائيًا إلى خارج أنظمة التجاري الداخلية.
- يجب ألا تتضمن الاتصالات الإلكترونية أي تزوير لهوية المُرسِل أو انتحال لاسم الشركة.
- يتحمل الموظفون المسؤولية الكاملة عن الحسابات المخصصة لهم وعن جميع الإجراءات التي تتم من خلالها.
- لا يجوز مشاركة الحسابات من دون تفويض مسبق من قسم تقنية المعلومات بالشركة، ويُستثنى من ذلك وظائف التقويم والمهام المرتبطة به.
- لا يجوز للموظفين استخدام حسابات البريد الإلكتروني الشخصية لإرسال أو استقبال المعلومات السرية الخاصة بالشركة.
- أي استخدام شخصي للبريد الإلكتروني المقدم من الشركة يجب ألا:
  - يتضمن أنشطة دعائية أو تسويقية.
  - يضر بسمعة التجارية.
  - يشمل إعادة إرسال رسائل تسلسلية.
  - يحتوي على أو يروّج لسلوكيات غير اجتماعية أو غير أخلاقية.
  - يؤدي إلى إفصاح غير مصرح به عن معلومات الشركة السرية.
  - يجب على الموظفين إرسال المعلومات السرية فقط باستخدام حلول مراسلة إلكترونية آمنة.
  - يجب توخي الحذر عند الرد على الرسائل الإلكترونية أو النقر على الروابط المرفقة بها أو فتح المرفقات المصاحبة لها.
- يجب على الموظفين التحلي بالحرص عند تضمين معلومات سرية أو داخلية في رسائل الرد التلقائي أو أي ردود آلية أخرى، مثل بيانات التوظيف أو أرقام الهواتف الداخلية أو مواقع العمل أو أي بيانات حساسة أخرى.

2.9 سياسة الأجهزة والبرمجيات

- يجب الحصول على موافقة رسمية من إدارة تقنية المعلومات قبل توصيل أي جهاز بالشبكات الخاصة بشركة التجارية.
- يجب أن تتم الموافقة على أي برمجيات يتم تثبيتها على أجهزة الشركة من قبل إدارة تقنية المعلومات، وأن يقوم موظفو قسم تقنية المعلومات حصريًا بعملية التثبيت.
- يجب تأمين جميع أصول الشركة التي يتم إخراجها خارج مقراتها بشكل مادي في جميع الأوقات.
- يجب على الموظفين الذين يسافرون إلى مواقع عالية المخاطر (وفقًا لتعريف الحكومة الكويتية) التواصل مع قسم تقنية المعلومات للحصول على موافقة مسبقة على السفر مع أصول الشركة.
- لا يجوز للموظفين السماح لأفراد الأسرة أو لأي أشخاص غير موظفين بالوصول إلى موارد المعلومات الخاصة بالشركة.

2.10 سياسة الإنترنت

- يُحظر استخدام الإنترنت لنقل معلومات سرية أو داخلية تخص شركة التجارية (التجارية) ما لم يتم ضمان سرية وسلامة هذه المعلومات والتأكد من هوية المستلم/المستلمين.
- يجب أن يقتصر استخدام الإنترنت من خلال موارد الشبكات أو الحوسبة الخاصة بالشركة على الأنشطة المرتبطة بالعمل فقط. وتشمل الأنشطة غير المصرح بها – على سبيل المثال لا الحصر – ما يلي:
  - الألعاب الترفيهية.
  - بث الوسائط.
  - استخدام وسائل التواصل الاجتماعي الشخصية.
  - الوصول إلى أو توزيع المواد الإباحية أو ذات الطابع الجنسي.
  - محاولة أو القيام بالدخول غير المصرح به إلى أي شبكة أو جهاز حاسوب متاح عبر الإنترنت.
- يجب أن يخضع الوصول إلى الإنترنت من خارج شبكة الشركة باستخدام أجهزة مملوكة للشركة لنفس السياسات المطبقة على الاستخدام من داخل مرافق الشركة.

2.11 سياسة الأجهزة المحمولة وسياسة إحضار جهازك

- لا تسمح شركة التجارية (التجارية) بتوصيل الأجهزة المحمولة المملوكة شخصيًا بالشبكة الداخلية للشركة.

أو

- يُعتبر استخدام جهاز محمول مملوك شخصيًا للاتصال بشبكة الشركة امتيازًا يُمنح للموظفين فقط بعد الحصول على موافقة رسمية من إدارة تقنية المعلومات.
- يجب أن تحتوي جميع الحواسيب المحمولة و/أو محطات العمل المملوكة شخصيًا على برامج معتمدة للكشف عن الفيروسات وبرامج التجسس/مكافحتها، بالإضافة إلى تفعيل جدار حماية شخصي.
- يجب أن تحتوي الأجهزة المحمولة التي تصل إلى البريد الإلكتروني للشركة على رقم تعريف شخصي (PIN) أو أي آلية مصادقة أخرى مفعلة.
- يجب تخزين البيانات السرية فقط على الأجهزة المشفّرة وفقًا لمعيار التشفير المعتمد من الشركة.
- يُحظر تخزين المعلومات السرية الخاصة بالشركة على أي جهاز محمول مملوك شخصيًا.
- يجب الإبلاغ فورًا إلى فريق أمن المعلومات في الشركة عن أي سرقة أو فقدان لجهاز محمول تم استخدامه لإنشاء أو تخزين أو الوصول إلى معلومات سرية أو داخلية.
- يجب أن يتم تحديث جميع الأجهزة المحمولة بانتظام لضمان أحدث إصدارات البرمجيات والتطبيقات.
- يتعين على جميع الموظفين استخدام الأجهزة المحمولة بطريقة أخلاقية ومسؤولة.
- يُحظر استخدام الأجهزة المكسورة الحماية (Jail-broken) أو المُجذّرة (Rooted) للاتصال بموارد المعلومات الخاصة بالشركة.
- يجوز لإدارة تقنية المعلومات بالشركة تنفيذ خاصية المسح عن بُعد للبريد الإلكتروني على الأجهزة المحمولة من دون سابق إنذار.
- في حال الاشتباه بوقوع حادث أو خرق متعلق بجهاز محمول، قد يكون من الضروري سحب الجهاز من حيازة الموظف كجزء من تحقيق رسمي.
- قد تتم مراقبة جميع استخدامات الأجهزة المحمولة المرتبطة بموارد معلومات الشركة وفقًا لتقدير إدارة تقنية المعلومات.
- يقتصر دعم قسم تقنية المعلومات على مساعدة الموظفين في الالتزام بهذه السياسة للأجهزة المملوكة شخصيًا، ولا يشمل ذلك حل المشكلات المتعلقة باستخدام الجهاز.
- يجب أن يتوافق استخدام الأجهزة المملوكة شخصيًا مع جميع السياسات الأخرى للشركة.

- تحتفظ الشركة بالحق في إلغاء امتيازات استخدام الأجهزة المحمولة المملوكة شخصيًا في حال عدم التزام الموظفين بالمتطلبات المنصوص عليها في هذه السياسة.
- يُحظر إرسال الرسائل النصية أو رسائل البريد الإلكتروني أثناء القيادة خلال وقت العمل أو عند استخدام موارد الشركة. ويُسمح فقط بالمكالمات باستخدام وضع التحدث الحر (Hands-Free) أثناء القيادة خلال وقت العمل أو عند استخدام موارد الشركة.

2.12 سياسة الأمن المادي

- يُحظر استخدام معدات التصوير أو التسجيل بأنواعها (الفيديو، الصوت، أو غيرها) بما في ذلك الكاميرات المدمجة في الأجهزة المحمولة داخل المناطق المؤمّنة.
- يتعين على الموظفين إبراز بطاقة الهوية الممغنطة المخصصة للدخول في جميع الأوقات أثناء وجودهم داخل المبنى.
- يجب على الموظفين استخدام بطاقات الدخول والخروج عند المرور بالمناطق الخاضعة للتحكم في الوصول. ويُحظر تمامًا ممارسات مثل الدخول المزدوج أو تثبيت الأبواب مفتوحة أو أي نشاط يهدف إلى التحايل على ضوابط التحكم في الدخول.
- يجب أن يكون الزوار الذين يدخلون إلى المناطق الخاضعة للتحكم بالبطاقات بصحبة موظفين مخوّلين في جميع الأوقات.
- يُحظر الأكل أو الشرب داخل مراكز البيانات. ويجب توخي الحذر عند الأكل أو الشرب بالقرب من محطات العمل أو مرافق معالجة المعلومات

2.13 سياسة الخصوصية

- المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها على موارد المعلومات الخاصة بشركة التجارية لا تُعتبر معلومات خاصة، وقد يتم الوصول إليها من قبل موظفي قسم تقنية المعلومات بالشركة في أي وقت، بتوجيه من الإدارة التنفيذية و/أو إدارة الموارد البشرية، ومن دون علم المستخدم أو مالك المورد.
- يجوز لشركة التجارية تسجيل أو مراجعة أو استخدام أي معلومات يتم تخزينها على أنظمة موارد المعلومات الخاصة بها أو تمر عبرها.
- قد يتمتع مسؤولو الأنظمة وموظفو تقنية المعلومات في الشركة، وغيرهم من الموظفين المخوّلين، بصلاحيات تتجاوز تلك الممنوحة للموظفين العاديين. وعلى الموظفين الحاصلين على هذه الصلاحيات الموسعة عدم الوصول إلى الملفات و/أو أي معلومات أخرى ما لم يكن ذلك ضروريًا بشكل محدد لتنفيذ مهام مرتبطة بالعمل.

2.14 سياسة الوسائط القابلة للإزالة

- يجب أن يكون استخدام الوسائط القابلة للإزالة لتخزين معلومات شركة التجارية) التجارية (مدعومًا بمبرر عملي معقول.
- يجب الحصول على موافقة مسبقة من قسم تقنية المعلومات في الشركة قبل استخدام أي وسائط قابلة للإزالة.
- يُحظر استخدام الوسائط القابلة للإزالة المملوكة شخصيًا لتخزين معلومات الشركة.
- لا يُسمح للموظفين بتوصيل أي وسائط قابلة للإزالة ذات مصدر غير معروف من دون موافقة مسبقة من قسم تقنية المعلومات في الشركة.
- لا يجوز تخزين المعلومات السرية أو الداخلية الخاصة بالشركة على وسائط قابلة للإزالة من دون استخدام التشفير.
- يجب الإبلاغ فورًا إلى قسم تقنية المعلومات عن أي فقدان أو سرقة لجهاز وسائط قابلة للإزالة قد يحتوي على معلومات تخص الشركة.

2.15 سياسة التدريب والتوعية الأمنية

- يجب على جميع الموظفين الجدد إتمام دورة تدريبية معتمدة للتوعية بأمن المعلومات قبل منحهم حق الوصول إلى أي من موارد المعلومات الخاصة بشركة التجارية، أو في غضون 30 يومًا كحد أقصى من تاريخ منحهم هذا الحق.
- يجب تزويد جميع الموظفين بالسياسات الخاصة بأمن المعلومات في الشركة، والتأكد من إقرارهم باستلامها وموافقتهم على الالتزام بها، وذلك قبل منحهم صلاحية الوصول إلى موارد المعلومات الخاصة بالشركة.
- يجب على جميع الموظفين إتمام التدريب السنوي للتوعية بأمن المعلومات.

2.16 سياسة وسائل التواصل الاجتماعي

- يجب أن تكون جميع الاتصالات المتعلقة بوسائل التواصل الاجتماعي متوافقة مع السياسات المعمول بها في شركة التجارية.
- يتحمل الموظفون المسؤولية الشخصية عن المحتوى الذي ينشرونه عبر الإنترنت.
- يتطلب إنشاء أي حساب عام على وسائل التواصل الاجتماعي يُقصد به تمثيل الشركة – بما في ذلك الحسابات التي قد يُفترض بشكل معقول أنها حسابات رسمية للشركة – الحصول على موافقة مسبقة من إدارة الاتصالات في الشركة.
- عند مناقشة موضوعات تخص الشركة أو مرتبطة بها، يجب على الموظف أن:
  - يعرّف بنفسه بالاسم.
  - يوضح أنه ممثل لشركة التجارية.
  - يبين بوضوح أنه يتحدث باسمه الشخصي وليس نيابة عن الشركة، ما لم يكن قد حصل على موافقة صريحة للقيام بذلك
- يجب على الموظفين عدم تحريف دورهم الوظيفي في الشركة.
- عند نشر محتوى له صلة بالشركة عبر الإنترنت بصفة شخصية، يجب أن يكون مصحوبًا بإخلاء مسؤولية. مثال على ذلك: "الآراء والمحتوى تعبر عن وجهة نظري الشخصية ولا تمثل بالضرورة موقف أو رأي شركة التجارية".
- يجب ألا ينتهك المحتوى المنشور عبر الإنترنت أي قوانين سارية (مثل قوانين حقوق النشر، أو الاستخدام العادل، أو الإفصاح المالي، أو قوانين الخصوصية).
- يُحظر نشر المعلومات السرية أو الاتصالات الداخلية أو المعلومات المالية أو التشغيلية غير المعلنة للشركة بأي شكل عبر الإنترنت.
- يُحظر نشر المعلومات الشخصية الخاصة بالعملاء عبر الإنترنت.
- يجب على الموظفين المخوّلين بالنشر أو المراجعة أو اعتماد المحتوى على حسابات الشركة في وسائل التواصل الاجتماعي الالتزام بالإجراءات المعتمدة لوسائل التواصل الاجتماعي الخاصة بالشركة.

2.17 سياسة البريد الصوتي

- يجب على الموظفين التحلي بالحرص عند تضمين معلومات سرية أو داخلية في رسائل الترحيب الخاصة بالبريد الصوتي، مثل بيانات التوظيف أو أرقام الهواتف الداخلية أو معلومات المواقع أو أي بيانات حساسة أخرى.

2.18 سياسة الاستخدام العرضي

- كخدمة تيسيريه لموظفي شركة التجارية، يُسمح بالاستخدام العرضي لموارد المعلومات. وتُطبق القيود التالية:
- يقتصر الاستخدام الشخصي العرضي لوسائل الاتصالات الإلكترونية، والوصول إلى الإنترنت، وأجهزة الفاكس، والطابعات، وآلات النسخ، وما شابه ذلك، على موظفي الشركة المعتمدين فقط؛ ولا يمتد ليشمل أفراد الأسرة أو المعارف الآخرين.
- يجب ألا يؤدي الاستخدام العرضي إلى تكاليف مباشرة على الشركة.
- يجب ألا يتعارض الاستخدام العرضي مع الأداء الطبيعي لمهام عمل الموظف.
- يُحظر إرسال أو استقبال أي ملفات أو مستندات قد تؤدي إلى اتخاذ إجراءات قانونية ضد الشركة أو عملائها أو تسبب لهم حرجًا.
- يجب أن يظل تخزين رسائل البريد الإلكتروني الشخصية، أو الرسائل الصوتية، أو الملفات، أو المستندات ضمن موارد المعلومات الخاصة بالشركة في حدود ضئيلة جدًا.
- جميع المعلومات الموجودة على موارد المعلومات الخاصة بالشركة تعتبر ملكًا لها، وقد تخضع لطلبات الإفصاح الرسمية، ويجوز الوصول إليها وفقًا لهذه السياسة.

استخدام أدوات الذكاء الاصطناعي الخارجية / العامة

- يُسمح باستخدام أدوات وخدمات الذكاء الاصطناعي (AI) الخارجية أو العامة لأغراض الإنتاجية التجارية فقط (مثل: إعداد المسودات، التلخيص، توليد الأفكار العامة) بطريقة لا تكشف أي معلومات سرية أو متعلقة بالعملاء أو شخصية أو مالية أو تعاقدية أو تصميمية أو رسومات/نماذج أو عروض أسعار أو أي معلومات حساسة أخرى.
- يُحظر على المستخدمين إدخال، أو رفع، أو لصق، أو الكشف بأي طريقة عن بيانات "سرية"، أو "سرية للغاية"، أو بيانات العملاء أو البيانات الشخصية في أدوات الذكاء الاصطناعي الخارجية. يجب أن يتم تنقية البيانات وإخفاء الهوية لمنع التعرف على الأفراد أو المشاريع أو الأطراف المقابلة أو التفاصيل الملكية عند الحاجة للسياق التجاري.
- يجب مراجعة والتحقق من مخرجات أدوات الذكاء الاصطناعي من قبل مستخدم ذو خبرة، ولا يجوز اعتبارها موثوقة دون التحقق منها.
- يجب على المستخدمين الالتزام بمتطلبات الترخيص وحقوق النشر والإفصاح المتعلقة بالمحتوى الناتج عن الذكاء الاصطناعي، كما هو محدد من قبل الإدارة القانونية وأمن المعلومات.

3. إدارة أمن المعلومات وعمليات تقنية المعلومات

3.1 التحكم في التغييرات

الغرض

يتمثل الغرض من سياسة التحكم في التغييرات في وضع القواعد الخاصة بإنشاء وتقييم وتنفيذ وتتبع التغييرات التي يتم إجراؤها على موارد المعلومات الخاصة بشركة التجارية.

النطاق المستهدف

تنطبق سياسة التحكم في التغييرات على أي فرد أو جهة أو عملية تقوم بإنشاء أو تقييم أو تنفيذ تغييرات على موارد المعلومات الخاصة بشركة التجارية.

السياسة

- يجب توثيق وتصنيف جميع التغييرات التي يتم إجراؤها على موارد المعلومات الإنتاجية الخاصة بشركة التجارية وفقًا الي ما يلي:
  - الأهمية.
  - درجة الاستعجال.
  - التأثير.
- يجب أن يتضمن توثيق التغييرات، كحد أدنى، ما يلي:
  - تاريخ تقديم طلب التغيير وتاريخ تنفيذه.
  - مالك التغيير والجهة المسؤولة عن حفظه.
  - طبيعة التغيير.
  - مقدم طلب التغيير.
  - تصنيف/تصنيفات التغيير.
  - خطة التراجع (Roll-back Plan).
  - الجهة المعتمِدة للتغيير.
  - منفذ التغيير.
  - مؤشر يوضح نجاح التغيير أو فشله.
- يجب جدولة التغييرات ذات التأثير المحتمل الكبير على موارد المعلومات في بيئة الإنتاج.
- يجب إخطار مالكي موارد المعلومات بأي تغييرات تؤثر على الأنظمة الواقعة ضمن نطاق مسؤولياتهم.
- يجب تحديد نوافذ تغيير معتمدة للتغييرات ذات التأثير العالي المحتمل.
- يجب أن تتضمن التغييرات ذات التأثير الكبير المحتمل و/أو التعقيد العالي اختبارات للاستخدام والأمن والتأثير، بالإضافة إلى خطط تراجع، ضمن وثائق التغيير.
- يجب حفظ وثائق التحكم في التغييرات وفقًا لجدول الاحتفاظ بالمعلومات المعتمد.
- يجب اعتماد جميع التغييرات من قبل مالك العمل أو مدير إدارة تقنية المعلومات أو لجنة التحكم في التغييرات.
- يجوز تنفيذ التغييرات الطارئة التي تتطلب تطبيقًا فوريًا (مثل الإصلاحات العاجلة أو الاستجابة للحوادث) من دون اتباع عملية التحكم في التغييرات الرسمية، إلا أنه لا يجوز بأي حال من الأحوال إهمال متطلبات التوثيق، حتى وإن تم التوثيق بعد تنفيذ التغيير.

3.2 الفصل بين المهام

- يجب ألا تكون الأطراف التي تمنح التفويض أو تقدم الطلب هي نفسها الأطراف المخوّلة بتنفيذ الإجراء، وذلك لضمان وجود نظام رقابة داخلية فعّال وتقليل مخاطر سوء استخدام النظام سواء عن طريق الإهمال أو التعمد. وتتحمل مسؤولية ضمان الفصل الكافي بين المهام كلٌّ من مديري الأقسام و/أو مالكي الخدمات. وتشمل الأنشطة والوظائف التي تتطلب بشكل أساسي الفصل بين المهام، على الأقل، ما يلي:
  - أ- تحديث الملفات الرئيسية وملفات المعايير.
  - ب- اعتماد وإدخال المدفوعات في أي نظام مالي.
  - ت- تسوية المعاملات المالية.
  - ث- إعداد التقارير المالية.
  - ج- إدارة الأنظمة.
  - ح- التدقيق الأمني.
  - خ- تطوير وصيانة الأنظمة.
- في الحالات التي يتعذر فيها تطبيق الفصل بين المهام، يجب تنفيذ ضوابط تعويضية إضافية.
- يتعين على الإدارة التأكد من أن الفصل المناسب بين المهام مطبَّق في جميع المجالات المتعلقة بتطوير الأنظمة وتشغيلها أو إدارتها.

3.3 الفصل بين بيئات التطوير والاختبار والإنتاج

- يجب أن تكون بيئتا التطوير والاختبار معزولتين على الأقل بشكل منطقي عن بعضهما البعض، مع تطبيق ضوابط محددة لأمن المعلومات لضمان سلامة كل منهما.
- لا يجوز للمختبرين والمطورين امتلاك معرفات مستخدم على أنظمة الإنتاج (باستثناء معرفات جدار الحماية التي يتم تفعيلها فقط من قبل موظفي تقنية المعلومات المخوّلين لدعم الموظفين في أغراض محددة). وفي حال تطلب الأمر وصولًا بعد الانتهاء من تطوير واختبار أنظمة المعلومات، يجب إنشاء معرفات مستخدم عادية أو ذات صلاحيات عليا للمطورين والمختبرين.
- يجب أن يقتصر وصول المطورين والمختبرين على الأجزاء اللازمة فقط من أنظمة المعلومات لأداء مهامهم، على أن يتم إلغاء هذا الوصول قبل انتقال النظام إلى بيئة الإنتاج.
- يجب أن تكون بيانات الإنتاج متاحة فقط في أنظمة الإنتاج. ويجب استخدام بيانات تجريبية في بيئات التطوير والاختبار كلما أمكن ذلك. وإذا كان من الضروري استخدام بيانات الإنتاج، فيجب أولًا إخفاء الحقول التي تحتوي على بيانات عالية الحساسية.
- يجب أن تحتوي بيئة الاختبار على تكوينات مماثلة لبيئة الإنتاج المقابلة، بحيث يمكن تحليل النتائج والتأثير على بيئة الإنتاج بدقة.
- لا يجوز نقل البيانات من بيئة إلى أخرى من دون موافقة رسمية من مالك الخدمة وقسم أمن المعلومات.
- يجب أن توضح الرسائل المعروضة على الشاشة أو ألوان الشاشة بشكل صريح ما إذا كان النظام نسخة اختبارية أو إنتاجية، وذلك لتقليل مخاطر إدخال معاملات اختبارية عن طريق الخطأ في أنظمة الإنتاج.
- يتعين على قسم تقنية المعلومات مراجعة الضوابط أعلاه بشكل دوري وإبلاغ قسم أمن المعلومات في حال وجود أي حالة عدم امتثال.

3.4 تخطيط السعة

- يتعين على قسم أمن المعلومات مراقبة وضبط استخدام موارده. يجب على قسم أمن المعلومات التنبؤ بالاحتياجات المستقبلية من السعة الخاصة بموارد أمن المعلومات، استنادًا إلى مدى أهمية الأعمال، وذلك لضمان تحقيق الأداء المطلوب للنظام.

3.5 التحكم في الثغرات التقنية

- يجب الحصول على المعلومات المتعلقة بالثغرات التقنية في أنظمة المعلومات المستخدمة بشكلٍ دوري وفي الوقت المناسب، وتقييم مستوى التعرض لهذه الثغرات، واتخاذ التدابير المناسبة إما لقبول المخاطر المرتبطة بها أو معالجتها.
- تكون إدارة البنية التحتية لتقنية المعلومات والعمليات، بالاشتراك مع مسؤول أمن المعلومات، مسؤولة عن مراقبة الثغرات، وتقييم المخاطر، وتطبيق التصحيحات، وتتبع الأصول، والتنسيق فيما بينها.
- تتحمل إدارة البنية التحتية لتقنية المعلومات والعمليات مسؤولية الحفاظ على مصادر معلومات كافية بشأن الثغرات التقنية، بما في ذلك مورّدو تقنية المعلومات ومصادر موثوقة أخرى من أطراف ثالثة.
- اعتمادًا على مستوى المخاطر ودرجة الاستعجال، يجب اتباع إجراءات إدارة التغييرات العادية أو التغييرات الطارئة أو إجراءات الاستجابة لحوادث أمن المعلومات في حال اكتشاف ثغرات تقنية.
- لا يجوز تطبيق أي تصحيح لمعالجة ثغرة تقنية إلا بعد أن يقوم مالك الخدمة بتقييم المخاطر المرتبطة بتطبيقه. وإذا تَبيَّن أن تطبيق التصحيح قد يُدخل مخاطر جديدة، فيجب تطبيق ضوابط تعويضية بديلة.
- يجب الحصول على التصحيحات فقط من مصادر موثوقة، وإذا لم تكن الحاجة عاجلة، فيُستحسن تطبيقها على دفعات.
- يجب تنفيذ أداة آلية لفحص الثغرات والامتثال للكشف الفوري عن الثغرات ومعالجتها، أو يمكن الاستعانة بمصادر خارجية لتنفيذ هذه الوظيفة بشكل دوري.

3.6 الحماية من الفيروسات

- يتعين على قسم تقنية المعلومات تثبيت برنامج مكافحة فيروسات معتمد على منصات تقنية المعلومات ذات الصلة. ويجب تكوين البرنامج لتحقيق الحماية المثلى وتحديثه فورًا عند صدور تحديثات لقاعدة بيانات الفيروسات وآليات الحماية.
- يجب فحص رسائل البريد الإلكتروني والمرفقات بشكل روتيني وآلي للكشف عن البرمجيات الخبيثة قبل فتحها.
- يجب أن تكون جميع أجهزة الحاسوب المكتبية والمحمولة مزودة ببرامج مكافحة فيروسات محدثة باستمرار..

3.7 أمن البرمجيات

- يجب اعتماد متطلبات البرمجيات الجديدة أو الإضافية من قبل مدير القسم المختص حيث يتم طلب البرمجيات. ويشمل ذلك جميع أنواع البرامج مثل البرمجيات التجارية، وبرامج أنظمة التشغيل، والأدوات المساعدة، والبرامج المجانية أو المشاركة، وبرامج التقييم.

- يجب أن يتم أي تثبيت لبرمجيات جديدة على أنظمة شركة التجارية) التجارية (بموافقة قسم تقنية المعلومات وقسم أمن المعلومات. ويُحظر تثبيت أي برمجيات غير معتمدة. كما يتعين على قسم تقنية المعلومات مراجعة وتقييم البرمجيات المطلوبة لضمان توافقها، في حين يتولى مسؤول أمن المعلومات التحقق من أن البرنامج لن يتسبب في إدخال ثغرات أمنية أو زيادة التهديدات الأمنية.

- يجب أن يقوم مسؤول أمن المعلومات وإدارة البنية التحتية لتقنية المعلومات والعمليات بتحديد التهديدات الناشئة من البرمجيات الخبيثة أو التهديدات الأمنية الأخرى باستخدام مصادر موثوقة مثل المواقع الإلكترونية المتخصصة في أمن المعلومات والتقنية، والمجلات المهنية، والاستشارات المتخصصة بشأن تطبيق الضوابط الأمنية المناسبة.

- يجب على قسم تقنية المعلومات، بالتشاور مع قسم أمن المعلومات، أن يحافظ على مكتبة برمجيات معتمدة (Definitive Software Library - DSL)، بحيث يقابل كل إدخال فيها إدخالًا في فهرس البرمجيات. كما يجب الحفاظ على نسخة احتياطية من مكتبة البرمجيات.

- يجب الحصول على صور البرمجيات (Software Images) في مكتبة DSL من مصادر موثوقة وأن تخضع لاختبارات أمنية.

- يُسمح فقط للشبكات المعتمدة ولمسؤولي البنية التحتية لتقنية المعلومات والعمليات بالوصول إلى مكتبةDSL ، مع الحفاظ على سجلات الدخول والاستخدام.

- يجب على قسم تقنية المعلومات الحفاظ على حالة أنظمة المعلومات محدثة باستمرار في فهرس البرمجيات، ويجب على قسم أمن المعلومات التحقق من ذلك عبر إجراء فحوصات دورية لا تقل عن مرة واحدة كل ثلاثة أشهر.

- يجب إدارة صور البرمجيات في مكتبة DSL بشكل مناسب، ولا يجوز إزالة الإصدارات القديمة إلا بعد التأكد من أنها لم تعد مطلوبة.

- لا يجوز الوصول إلى مكتبات البرامج التشغيلية أو مكتبات الشيفرات المصدرية إلا من قبل الموظفين المصرح لهم. ويجب ألا تُجرى التعديلات إلا باستخدام مزيج من ضوابط الوصول التقنية وإجراءات قوية يتم تنفيذها تحت إشراف مزدوج.(Dual Control)

- يجب تجنّب التعديلات الطارئة على البرمجيات إلا في الحالات التي تحددها الإدارة مسبقًا باعتبارها "حرجة". وفي جميع الأحوال، يجب أن تخضع مثل هذه التعديلات لعملية التحكم في التغييرات المتفق عليها بشكل صارم.

3.8 الحماية من البرمجيات الخبيثة

- يجب تكوين الأجهزة الواقعة على حدود الشبكة الأساسية بطريقة تمنع انتشار البرمجيات الخبيثة إلى خارج الشبكة.
- يجب الحصول على حلول مكافحة البرمجيات الخبيثة من عدة مزوّدين ونشرها، وذلك لضمان الحماية من البرمجيات الخبيثة التي قد لا يتم اكتشافها بواسطة أداة فحص واحدة.
- يجب فحص الوسائط القابلة للإزالة للتأكد من خلوها من البرمجيات الخبيثة قبل نقل أي معلومات إليها.
- يجب عزل أي نظام معلومات أو جهاز أو شبكة تُصاب ببرمجيات خبيثة على الفور.
- يجب إعداد تقرير يوضح بالتفصيل أداء حلول مكافحة البرمجيات الخبيثة التي تم تطبيقها.
- يجب الحفاظ على صورة رئيسية للأنظمة الحيوية ذات الأهمية، بحيث يمكن استخدامها لاستعادة النظام في حال تعذر إزالة البرمجيات الخبيثة.

3.9 الحماية من تهديدات الشيفرات الخبيثة

- يجب تحديد التهديدات الأمنية المرتبطة بالشيفرات الخبيثة وتقييمها، واتخاذ الإجراءات اللازمة للتخفيف منها عند الضرورة.
- يجب وضع وتنفيذ إجراءات للتعامل مع الشيفرات الخبيثة.
- يجب على إدارة البنية التحتية لتقنية المعلومات والعمليات مراقبة التحديثات الأمنية المتعلقة بثغرات الشيفرات الخبيثة بشكل دوري، ورفع تقارير عنها إلى مسؤول أمن المعلومات الذي يتولى بدوره اتخاذ الإجراءات المناسبة.
- يجب حجب الشيفرات الخبيثة غير المصرح بها ومنع تنزيلها و/أو تنفيذها. كما يجب تصميم أنظمة المعلومات بطريقة تولد رسائل تحذيرية قبل تنفيذ أي شيفرة مصرح بها.
- يجب تقييد تنفيذ الشيفرات الخبيثة "المصرح بها" ليقتصر على بيئات معزولة منطقيًا) مثل :

3.10 النسخ الاحتياطي للمعلومات

- يتعين على شركة التجارية وضع إجراء للنسخ الاحتياطي يحدد متطلبات الاحتفاظ والحماية الخاصة بالنسخ الاحتياطية، وأخذ نسخ احتياطية من المعلومات والبرمجيات وصور الأنظمة.
- يجب على مالك نظام المعلومات التأكد من وجود إجراءات كافية للنسخ الاحتياطي واستعادة النظام.
- يُعتبر النسخ الاحتياطي لملفات بيانات الشركة وضمان القدرة على استعادتها أولوية قصوى. ويتحمل مالكو البيانات والإدارة مسؤولية ضمان أن وتيرة عمليات النسخ الاحتياطي وإجراءات الاستعادة تلبي احتياجات الأعمال.
- يجب أن تكون وسائط التخزين المستخدمة في أرشفة المعلومات مناسبة للعمر الافتراضي المتوقع لها. كما يجب النظر بعناية في صيغة تخزين البيانات وتوثيقها، خاصة في الحالات التي تُستخدم فيها صيغ خاصة .
- يجب أن تعكس عملية أرشفة الملفات الإلكترونية احتياجات العمل والمتطلبات القانونية والتنظيمية.
- يجب على الإدارة التأكد من وجود الضمانات الكفيلة بحماية سلامة ملفات البيانات أثناء عملية الاستعادة وإعادة التشغيل.

3.11 تبادل المعلومات

- يجب حماية المعلومات المتبادلة بشكل مناسب من الاعتراض أو النسخ أو التعديل أو التحويل الخاطئ أو الإتلاف، وذلك وفقًا لمستوى التصنيف ومخاطر الانتهاك.
- يجب استخدام مرافق الاتصالات الإلكترونية وفقًا للإرشادات المعمول بها وسياسات الاستخدام المقبول (يرجى الرجوع أيضًا إلى سياسة الاستخدام المقبول).
- يجب استخدام تقنيات التشفير المناسبة لحماية سرية المعلومات وسلامتها وأصالتها عند تبادلها، وذلك بما يتماشى مع سياسة تصنيف المعلومات. وفي الحالات التي يتعذر فيها استخدام تقنيات التشفير، يجب تطبيق ضوابط تعويضية مناسبة.
- يجب وضع اتفاقيات لتبادل المعلومات والبرمجيات بين شركة التجارية والجهات الأخرى. ويجب أن تتضمن هذه الاتفاقيات ما يلي:
  - أ- بنود السرية وبنود المسؤولية في العقود للحد من مسؤولية الشركة عن أي تسريب للمعلومات ناجم عن إخفاقات أمنية لدى جهات أخرى.
  - ب- ترتيبات الضمان، مثل تأمين الشيفرة المصدرية في حال تعرض مورّد البرمجيات للإفلاس، أو فقدان موظفين أساسيين، أو عجزه عن تقديم مستوى الدعم المطلوب.
  - ت- أحكام ملكية المعلومات والبرمجيات، والمسؤوليات المتعلقة بحماية البيانات والامتثال لحقوق النشر الخاصة بالبرمجيات.
- يجب اعتماد اتفاقيات الربط بين أنظمة المعلومات من قبل الإدارة العليا المختصة.
- يتعين على المسؤول عن إدارة الموارد البشرية التأكد من أن جميع الموظفين على دراية كاملة بواجباتهم القانونية والمؤسسية فيما يخص منع المشاركة أو الإفصاح غير المناسب عن المعلومات، سواء داخل الشركة أو مع الأطراف الخارجية.

3.12 الوسائط المادية أثناء النقل

- يجب استخدام وسائل نقل موثوقة أو خدمات بريدية/نقل معتمدة لنقل الوسائط المادية بين مقار الشركة والمواقع الأخرى. ويجب الاتفاق مع الإدارة العليا على قائمة الناقلين المعتمدين. كما يتعين إلزام الناقلين، بموجب عقد، بحماية الوسائط القابلة للإزالة والمعلومات المخزنة عليها من الوصول غير المصرح به أو النسخ أو السرقة.
- يجب أن تكون تغليفات الوسائط كافية لحماية المحتوى من التلف المادي أثناء النقل، وأن تتوافق مع مواصفات الشركات المصنعة (مثل حاويات الأشرطة المؤمنة والقابلة للإغلاق والمصممة خصيصًا لهذا الغرض).
- يجب تطبيق ضوابط أمنية إضافية لحماية الوسائط التي تحتوي على معلومات مصنفة بدرجة سرية عالية أو سرية من أي إفصاح أو تعديل غير مصرح به. ومن أمثلة هذه الضوابط: استخدام التشفير، الحاويات المقفلة، التسليم باليد، التغليف المقاوم للعبث، تقسيم الشحنة إلى أكثر من دفعة يتم إرسالها عبر مسارات مختلفة، والحصول على تأكيد استلام من الجهة المستقبلة.

3.13 المراسلات الإلكترونية وأمن الإنترنت

- يجب حماية المعلومات الحساسة المتداولة عبر المراسلات الإلكترونية بشكل مناسب وفقًا لمخاطر أمن المعلومات ومستوى تصنيفها.
- جميع رسائل البريد الإلكتروني الصادرة من حسابات البريد الإلكتروني الخاصة بموظفي الشركة تعتبر مملوكة لشركة التجارية وتخضع للرقابة.
- يجب إرسال المعلومات المصنفة بدرجة سرية أو أعلى فقط عبر البريد الإلكتروني الآمن.
- يجب أن تكون الرسائل الإلكترونية الصادرة مشفّرة كلما أمكن ذلك.
- يجب أن تتضمن الرسائل الإلكترونية الصادرة إخلاء مسؤولية.
- يتعين على قسم تقنية المعلومات ومسؤول أمن المعلومات توفير الأدوات اللازمة لمراقبة استخدام الإنترنت لجميع أجهزة الحاسوب والأجهزة المتصلة بالشبكة المؤسسية. ويجب أن يقوم نظام المراقبة بتسجيل عنوان الـ IP للمصدر، والتاريخ، والوقت، والبروتوكول، والموقع أو الخادم المستهدف لكل حركة مرور على الإنترنت. وحيثما أمكن، يجب أن يسجل النظام معرف المستخدم الخاص بالحساب الذي أنشأ الحركة. ويجب الاحتفاظ بسجلات استخدام الإنترنت لمدة 180 يومًا
- يجب على مسؤول أمن المعلومات مراجعة قواعد تصفية الويب والبروتوكولات بشكل دوري وتقديم التوصيات اللازمة بشأن تعديلها.أي تغييرات تُجرى على قواعد تصفية الويب والبروتوكولات يجب أن تنعكس في سياسة استخدام الإنترنت ضمن سياسات الاستخدام المقبول.
- يجب تعطيل إعادة توجيه بريد شركة التجارية تلقائيًا إلى حسابات خارجية افتراضيًا، ويُحظر ذلك إلا بعد الحصول على موافقة رسمية لسبب تجاري موثق.

3.14 التسجيل والمراقبة التدقيقية

- يجب تطبيق التسجيل التدقيقي على جميع مستويات الأنظمة ذات الصلة، بما في ذلك أجهزة الشبكة (وكذلك المنافذ التشخيصية)، وأنظمة التشغيل، والتطبيقات، والخوادم، وقواعد البيانات. كما يجب أن يتم تحديد السمات المطلوب تسجيلها، وتواتر التسجيل، ومدة الاحتفاظ، ومكان تخزين السجلات مسبقًا من قبل مالكي الخدمة لكل نظام.
- يجب حماية سجلات التدقيق وإعدادات التسجيل التدقيقي من الوصول غير المصرح به أو التعديل أو الحذف. ويجب أرشفة سجلات التدقيق وفقًا لمعايير الأرشفة المعتمدة لدعم التحقيق في الحوادث الأمنية وضمان المراقبة الأمنية الروتينية.
- يجب تنفيذ أنظمة وإجراءات لمراقبة استخدام مرافق معالجة المعلومات من خلال السجلات، وذلك للتأكد من أن المستخدمين لا يقومون بأنشطة غير مصرح بها أو غير ملائمة.
- يجب تحديد مستوى المراقبة المطلوب لكل نظام بشكل منفصل من قبل مالك الخدمة وقسم أمن المعلومات وإدارة المخاطر وقسم تقنية المعلومات، وذلك وفقًا لتصنيف النظام.

3.15 تسجيل ومراقبة أحداث الأمن

- حيثما يكون ذلك مناسبًا، يجب مراقبة أنظمة التسجيل وملفات السجلات بشكل مستمر للحماية من التغييرات غير المصرح بها والمشكلات التشغيلية مثل:
  - أ- تعطيل وظائف التسجيل الأمني.
  - ب- التعديلات على محتوى ملفات السجلات (سواء العرضي أو المتعمد) أو على تواريخ وأوقات الملفات أو الإدخالات الفردية.
  - ت- حذف أو إعادة تسمية ملفات السجلات.
  - ث- امتلاء مساحة ملفات السجلات بما يؤدي إلى تجاهل أو استبدال السجلات.
- يجب تتبع ومراقبة الوصول إلى بيانات العملاء.
- يجب نقل أنواع الرسائل ذات الصلة تلقائيًا إلى نظام تسجيل مركزي آمن، حيث يمكن دمج المعلومات من مصادر متعددة وتحليلها للمساعدة في تحديد الأحداث الهامة لأغراض المراقبة الأمنية.
- يجب مراجعة سجلات الأمن بشكل منتظم من قبل قسم أمن المعلومات، وعند الضرورة من قبل أطراف أخرى مخوّلة تحديدًا من الإدارة العليا. ويجب رفع أي نتائج رئيسية يتم تحديدها خلال المراجعة إلى الإدارة التنفيذية. كما يجوز لمالك الخدمة أو قسم أمن المعلومات أو إدارة التدقيق الداخلي مراجعة سجلات الأمن في أي وقت.
- يجب عرض نتائج المراجعة والتوصيات الناشئة عنها على هيئة حوكمة أمن المعلومات الخاصة بالشركة.

3.16 سجلات المشغلين

يجب الاحتفاظ بسجلات المشغلين التي تتضمن جميع سجلات المستخدمين المتعلقة بأنشطة الدعم الخاصة بالوصول الداخلي والخارجي.

3.17 تسجيل الأعطال

- يقصد بالأعطال، في سياق هذه السياسة، المشكلات المتعلقة بأنظمة تقنية المعلومات أو أنظمة الاتصالات، بما في ذلك حالات خرق الأمن المؤكدة أو المشتبه بها، تعطل الأنظمة، أخطاء/عيوب البرامج، الفيروسات، وأي عمليات أخرى غير مرغوبة في أنظمة المعلومات. يجب الإبلاغ عن الأعطال وتسجيلها باستخدام وظائف آلية متى ما كانت متوفرة.
- يجب اتخاذ إجراءات المراقبة الفورية والتدابير التصحيحية المناسبة بشكل عاجل عند الإبلاغ عن عطل. ويجب وضع قواعد واضحة للتعامل مع الأعطال المبلغ عنها، بما في ذلك مراجعات الإدارة للآتي:
  - أ- سجلات الأعطال للتأكد من معالجة الأعطال بشكل مرضٍ.
  - ب- التدابير التصحيحية لضمان عدم المساس بالضوابط وأن جميع الإجراءات المتخذة كانت مصرحًا بها بالكامل.
  - ت- معلمات تكوين تسجيل الأخطاء.

3.18 مزامنة الساعة

- يجب تكوين جميع الأنظمة، بما في ذلك الشبكات وأجهزة الأمن، لمزامنة الساعات مع خادم الوقت المعتمد من قبل الشركة.

3.19 الخوادم

- يجب تكوين أنظمة التشغيل بما يتوافق مع معايير أمن أنظمة التشغيل المعتمدة.
- يجب تعطيل الخدمات والتطبيقات المثبتة على الخوادم في حال عدم استخدامها.
- يجب تثبيت التصحيحات الأمنية الحرجة على خوادم التطوير والاختبار والإنتاج فور إصدارها، ما لم تتعارض هذه التصحيحات مع متطلبات الخدمة أو توافرها.
- يجب تسجيل الأحداث المتعلقة بالأمن (مثل الوصول والتغييرات) على الخوادم الحرجة، والاحتفاظ بسجلات التدقيق الخاصة بها.
- يجب توثيق معلومات الخادم والتكوين الأساسي للخوادم المحصّنة في قاعدة بيانات إدارة التكوين، كما يجب أن تخضع أي تغييرات في تكوين الخادم لإجراءات إدارة التغيير المعتمدة. ويجب أيضًا الحفاظ على مواصفات الأجهزة المعتمدة في وثائق رسمية.
- يجب أن تتوافق المهام التي تُنفذ على الخوادم مع مبادئ الأمن القياسية المتعلقة بمنح أقل مستوى من الوصول المطلوب.

3.20 الفصل بين الشبكات

- يجب فصل أنظمة وشبكات شركة التجارية الداخلية وفقًا لمخاطر أمن المعلومات المرتبطة بها إلى فئات أو مجموعات أو أقسام أو نطاقات منفصلة، كما هو موضح أدناه:
  - أ- الأنظمة المملوكة أو المُدارة من قبل مورّدين خارجيين مقابل أنظمة الشركة.
  - ب- الأنظمة التي تحتوي على بيانات مصنفة بدرجة سرية أو أعلى يجب أن تكون ضمن الشبكة الأساسية.
  - ت- بيئات التطوير مقابل الاختبار مقابل الإنتاج.
  - ث- الشبكات السلكية مقابل الشبكات اللاسلكية.
- يجب أن تكون الأنظمة المصنفة بدرجة سرية للغاية ضمن بيئة حوسبة مخصصة.
- يجب أن يعتمد الفصل على آليات تحكم مناسبة مثل الجدران النارية أو البوابات أو العزل المادي أو التشفير (مثل الشبكات الخاصة الافتراضية أو الشبكات المحلية الافتراضية، وذلك بما يعكس المتطلبات الأمنية الناشئة عن احتياجات الأعمال والمخاطر الأمنية المُقيَّمة.
- يجب تكوين الجدران النارية بشكل مناسب لحماية بيانات العملاء.
- يجب أن يسمح الجدار الناري عند حدود الشبكة بالاتصال فقط من شبكة يمكن التحقق من حالة جلستها (مثل بروتوكول التحكم بالنقل TCP أو بروتوكول بيانات المستخدم UDP).
- لحماية أنظمة ومعلومات الشركة الداخلية، يجب إنشاء مناطق منزوعة السلاح (DMZs) لوضع المعلومات المتاحة للعامة فيها.
- يجب رفض أي طلبات خارجية غير مصرح بها إلى أجهزة الشبكة.

3.21 ضوابط الشبكة

- يجب إدارة الشبكات والتحكم بها لضمان حمايتها من التهديدات الأمنية الداخلية والخارجية، ولحماية الأنظمة والتطبيقات والمعلومات التي تتم معالجتها على الشبكة.
- يجب إسناد مسؤوليات إدارة وتأمين شبكات التجارية) التجارية (والبنية التحتية العامة لتقنية المعلومات إلى إدارة البنية التحتية والعمليات (IT Infrastructure & Operations).كما يجب تنسيق ومراقبة أنشطة إدارة الشبكات والحواسيب لتقليل المخاطر على الأعمال وضمان تطبيق ضوابط أمن المعلومات بشكل متسق على مستوى البنية التحتية بأكملها.
- يجب أن تستخدم حدود الشبكة، وحيثما كان ذلك مناسبًا، النطاقات الداخلية المنفصلة، جدرانًا نارية (Firewalls) و/أو قوائم التحكم بالوصول على أجهزة التوجيه (Router ACLs) لمراقبة والتحكم بالوصول إلى الشبكات والأنظمة المتصلة بها واستخدامها.
- يجب تنفيذ آليات احتياطية لحدود الشبكة (Redundant Network Boundary Mechanisms) لتجنب تسرب المعلومات نتيجة لفشل آلية الحماية الأساسية لحدود الشبكة.
- يجب تحديد ميزات الأمان ومستويات الخدمة والمتطلبات الإدارية لخدمات الشبكة ذات الصلة (مثل توفير الاتصالات، وخدمات الشبكات الخاصة، والشبكات ذات القيمة المضافة، وحلول إدارة أمن الشبكات مثل الجدران النارية وأنظمة كشف التسلل) وتوثيقها والاتفاق عليها في اتفاقيات خدمات الشبكة.(Network Services Agreements)
- عند اختيار أنظمة كشف ومنع التسلل(IDPS) ، يجب أخذ بيئة تقنية المعلومات والأنظمة المعلوماتية ذات الصلة في الاعتبار. كما يجب تكوين أنظمة IDPS بحيث لا يؤدي ردها التلقائي على الهجمات إلى إدخال مخاطر إضافية.
- في حالة الشبكات المشتركة، وخاصة تلك الممتدة عبر حدود المنظمة، يجب تقييد قدرة المستخدمين على الاتصال بالشبكة. ويجب تطبيق سياسات تحكم بالوصول يمكن أن تستند إلى السمات أو الأدوار أو الهوية.
- يجب تطبيق ومراقبة الجدران النارية وضوابط توجيه حركة المرور الأخرى) مثل آليات التحقق من عناوين المصدر والوجهة، ونطاقات عناوين IPالداخلية المحددة، وترجمة عناوين الشبكة (NAT للتحكم في تدفق المعلومات داخل الشبكات العامة والداخلية أو فيما بينها.
- يجب تمكين النسخة المستقرة والآمنة من بروتوكول إدارة الشبكات البسيط (SNMP) على الأجهزة التي تتطلب ذلك.
- يجب تقليل احتمالية تعرض أجهزة الشبكات للهجمات من خلال تحصين الأجهزة الشبكية(Hardening) ، بما في ذلك تعطيل البروتوكولات أو الخدمات أو المنافذ غير الضرورية، ونشر أدوات لاكتشاف الهجمات المحتملة.
- يجب استخدام تقنيات الحماية) مثل تقييد حزم المزامنة SYN وحزم بروتوكول رسائل التحكم بالإنترنت (ICMP كوسيلة للحماية من هجمات حجب الخدمة.(DoS)
- يجب أن تسمح المحولات (Switches) بالوصول إلى منافذها فقط بناءً على عناوين التحكم بالوصول إلى الوسائط.(MAC Addresses)
- يجب فرض معيار الأمان الخاص بشركة التجارية) التجارية (Security Standard على جميع أجهزة الشبكة والأمن. كما يتعين على قسم تقنية المعلومات مراجعة الامتثال لهذه المعايير بشكل دوري وإبلاغ قسم أمن المعلومات (ISS) في حالة وجود أي عدم امتثال.

3.22 مصادقة معدات الشبكة

- يجب تعريف المكونات المادية لشبكة الشركة للنظام الذي يتم الوصول إليه. وقد تشمل هذه الأجهزة: المحطات الطرفية، الخطوط، عقد الاتصالات، محولات الشبكة، وحدات التحكم، المعالجات البعيدة، وأجهزة الحاسوب الشخصية. ويجب أن تكون طرق مصادقة العقد المختارة لتلبية متطلبات العمل والأمن مصممة بشكل احترافي، وموثقة، ومختبرة، ومطبقة، ومشغّلة، ومصانة، ويتم مراجعتها بشكل دوري، بحيث تعكس وتيرة وعمق المراجعة مستوى مخاطر الأمن.
- يجب أن تكون مكونات الشبكة قابلة للتعريف بشكل فريد، ومقيّدة بأداء وظائفها التجارية المخصصة فقط.

3.23 حماية منافذ التشخيص والإعدادات عن بُعد

- يجب التحكم في الوصول المادي والافتراضي إلى منافذ التشخيص والإعدادات، ولا يجوز تفعيل سوى المنافذ والخدمات والبروتوكولات اللازمة لأداء الخدمات المطلوبة.
- يجب أن يقتصر الوصول إلى منافذ التشخيص عن بُعد أو منافذ الإعدادات/الإدارة أو منافذ وحدة التحكم والمودمات التي تتيح وصولًا مميزًا للدعم الفني على الأجهزة مثل: مقاسم الهاتف، الخوادم، أنظمة الأقراص، الموجّهات، الجدران النارية ، والبوابات، على موظفي الدعم المصرح لهم والموردين الخارجيين فقط، وذلك باستخدام آليات قوية لمصادقة المستخدم والتحكم في الوصول. ولا يجوز أن تكون هذه المنافذ مفعلة بشكل افتراضي، ويجب إلغاء الوصول إليها فور انتهاء الحاجة لها.
- لا يجوز تفعيل المنافذ المميزة إلا عند الضرورة، ولأغراض أنشطة دعم محددة ومصرح بها عن بُعد.
- يجب تحديد وإغلاق المنافذ غير الضرورية من خلال عمليات مسح دورية لأجهزة الشبكة. علاوة على ذلك، يجب إجراء مراجعات منتظمة (مرة واحدة على الأقل كل 6 أشهر) للخدمات، ولا يجوز الإبقاء إلا على الخدمات التي يمكن تبرير تشغيلها.

3.24 أمن الشبكات اللاسلكية

- عند تصميم وتنفيذ ضوابط أمان الشبكات اللاسلكية، يجب القيام بما يلي:
  - إجراء مسح لتحديد المواقع المناسبة لتركيب نقاط الوصول.
  - يجب ألا تكشف معرّفات مجموعات الخدمة الخاصة بنقاط الوصول عن أي معلومات تخص شركة التجارية للمستخدمين الخارجيين للشبكة.
  - يُحظر إنشاء شبكات لاسلكية مؤقتة.
- يجب تعطيل طلبات الاتصال الواردة إلى الأجهزة المحمولة.
- يجب تكوين التشفير القوي على الشبكة اللاسلكية.
- يجب تقييد نقاط الوصول غير المعرّفة.
- عند الوصول إلى الشبكة الأساسية (Core Network) عبر نقاط الوصول اللاسلكية، يجب تطبيق نفس ضوابط المصادقة والتحكم في الوصول المطبقة على الشبكات السلكية.
- يجب ألا يمرر أي جزء من حركة مرور البيانات الخاصة بالشبكة الضيف (Guest Network) عبر الشبكة الأساسية.
- يجب تعطيل خيارات الاتصال اللاسلكي قصير المدى مثل البلوتوث (Bluetooth) والأشعة تحت الحمراء.(Infrared)
- يجب أن يقتصر الاتصال بشبكة الضيوف اللاسلكية على فترة زمنية محددة وفقًا لساعات عمل الشركة.
- إذا كان يتعين إرسال معلومات مصنفة بدرجة سرية أو أعلى عبر شبكة لاسلكية عامة، فيجب استخدام شبكة افتراضية خاصة.(VPN)
- يجب على الشركة تنفيذ عمليات اختبار دورية للكشف عن وجود نقاط الوصول اللاسلكية (802.11)، والتعرف على جميع نقاط الوصول المصرح بها وغير المصرح بها بشكل ربع سنوي.

3.25 أجهزة الحوسبة المحمولة

- يتعين تطبيق ضوابط الأمان المناسبة عند استخدام مرافق تكنولوجيا المعلومات المحمولة، مثل الحواسيب المحمولة/النقالة والهواتف المحمولة المزوّدة من قبل شركة التجارية، وذلك لضمان حماية أصول معلومات الشركة، بما في ذلك الأجهزة والبرمجيات والبيانات.
- تتحمّل إدارة تقنية المعلومات مسؤولية صيانة أنظمة التشغيل وبرمجيات التطبيقات، بما في ذلك تنفيذ التحديثات والتصحيحات الأمنية بشكل دوري وسريع لمعالجة الثغرات الأمنية الجوهرية، بالإضافة إلى تفعيل جدران الحماية الشخصية وبرامج الحماية من البرمجيات الخبيثة على الأجهزة المحمولة.
- يُسمح باستخدام أجهزة الحوسبة الخاصة بالشركة فقط من قبل الموظفين المخوّلين أو من قبل الموردين الخارجيين المتعاقدين مع الشركة، ويقتصر استخدامها على الأغراض المهنية المرتبطة بأنشطة العمل فقط.
- يجب أن يتم تهيئة الأجهزة والأنظمة المحمولة مسبقًا من قبل إدارة تقنية المعلومات، بما يشمل تطبيق ضوابط التحكم في الوصول، وتفعيل تقنيات التشفير، وضبط إعدادات الشبكة، وتوفير حلول النسخ الاحتياطي للبيانات، بالإضافة إلى أنظمة الحماية من الفيروسات.

3.26 استخدام الضوابط التشفيرية

- يجب استخدام التشفير لحماية المعلومات (سواء المستضافة داخليًا أو لدى طرف ثالث) التي تتطلب درجة عالية من السرية و/أو السلامة (النزاهة).
- عند تنفيذ أدوات التشفير في شركة التجارية، يجب مراعاة المتطلبات التالية:
  - أ- متطلبات التعامل مع المعلومات الحساسة عند نقلها باستخدام وسائط متنقلة أو قابلة للإزالة، أو عبر خطوط الاتصال.
  - ب- تأثير استخدام المعلومات المشفّرة على الضوابط الأمنية الأخرى (مثل كشف الفيروسات).
  - ت- يجب اختيار طول المفتاح التشفيري وفقًا لتصنيف المعلومات
- يجب تطبيق فقط الضوابط التشفيرية المعتمدة عند تقديم خدمات جديدة أو إجراء تعديلات على الخدمات الحالية.
- استنادًا إلى تصنيف المعلومات، يجب تشفير البيانات المخزنة على أجهزة الحواسيب المكتبية والمحمولة.
- يجب تشفير الأجهزة المحمولة في حال كانت تحتوي على معلومات مصنّفة بأنها "سرية" أو أعلى.
- يجب أن تضمن الضوابط التشفيرية تحقيق السرية والسلامة (النزاهة) وعدم الإنكار للرسائل التي تحتوي على بيانات المعاملات التجارية السرية.

3.27 البنية التحتية للمفتاح العام

- يجب مصادقة أنظمة المعلومات التي تطلب الوصول المباشر أو عبر وكيل باستخدام شهادة مفتاح عام، متى ما كان ذلك ممكنًا من الناحية الفنية. ويجب التحقق من صحة شهادة المفتاح العام قبل الارتباط بها. واعتمادًا على درجة الحماية/مستوى الثقة المطلوب من قبل العمل، يجب التحقق من التوقيعات الرقمية باستخدام مفاتيح عامة مخصصة للتوقيع وموثّقة على شهادات رقمية صادرة عن جهات إصدار شهادات موثوقة ومعتمدة.
- يجب تنفيذ التشفير سواء من خلال الأجهزة أو البرمجيات، حسب الاقتضاء، ويجب الحصول على موافقة قسم أمن المعلومات مسبقًا قبل استخدام أي منتجات أو عمليات أو معايير تشفير. سيتولى قسم أمن المعلومات مسؤولية الاحتفاظ بقائمة بجميع الخوارزميات المعتمدة وأطوال المفاتيح المقبولة.
- يجب على الشركة استخدام شهادات رقمية صادرة عن جهة إصدار شهادات معترف بها، ويجب أن تكون هذه الشهادات بمستوى ضمان لا يقل عن المستوى المتوسط كحد أدنى. وللاستخدامات الداخلية، يجوز للشركة استخدام شهادات رقمية صادرة عن جهة إصدار شهادات داخلية تابعة للشركة.
- تُعد الشهادات الرقمية إلزامية لجميع خوادم الإنترنت التي تقدم خدمات لعملاء أو شركاء شركة التجارية
- يجب استخدام الشهادات الرقمية داخليًا أيضًا على الأنظمة التي تنقل معلومات مصنفة على أنها سرية، مع الأخذ في الاعتبار تأثير التشفير على أداء النظام واستمرارية الأعمال.
- يجب الالتزام بأي متطلبات تنظيمية تتعلق بإنشاء واستخدام ومعالجة وإتلاف المفاتيح التشفيرية.
- يجب تحليل ومراجعة واعتماد استخدام التشفير في أي سياق أعمال من قبل قسم أمن المعلومات.
- يجب على إدارة تقنية المعلومات استخدام خوارزميات قياسية مثبتة فقط مثل AES :و RSAو IDEAكأساس لتقنيات التشفير. ولا يجوز استخدام أي خوارزميات تشفير مملوكة لم تخضع لتدقيق عام صارم.
- يجب حماية مفاتيح التشفير بعناية من قبل مالكيها أو القائمين على إدارتها، ولا يجوز تحت أي ظرف من الظروف مشاركتها مع أي طرف ثالث. كما يجب أن تكون المفاتيح السرية محمية بكلمة مرور.
- يجب توزيع المفاتيح العامة من خلال خدمة دليل مؤمّنة بشكل مناسب، وفي حال عدم توفر ذلك، يجوز للمستخدمين توزيع مفاتيحهم العامة بأنفسهم.
- يجب أن تكون فترة صلاحية المفتاح التشفيري معتمدة على الخوارزمية وطول المفتاح المستخدم. ويجب أن تتوافق هذه الفترة مع التوصيات المنشورة من الجهات المختصة و/أو الخبراء المستقلين.
- يجوز إلغاء المفاتيح قبل نهاية فترة صلاحيتها إذا تم اختراقها أو إساءة استخدامها، أو بناءً على طلب المستخدم.

- يجب إخطار المستخدم أو المسؤول تلقائيًا بقرب انتهاء صلاحية المفتاح قبل موعد الانتهاء.

3.28 أجهزة وبرمجيات الأمن السيبراني

- يجب أن يتم تنفيذ وصيانة الأجهزة والبرمجيات المتعلقة بأمن المعلومات من قبل أفراد مخولين ومدرّبين على ذلك.
- ويُقصر استخدام برمجيات الأمن السيبراني على الأفراد الذين تتطلب مهامهم الوظيفية استخدامها فقط.

3.29 صيانة الأجهزة

- يجب صيانة معدات وأجهزة تقنية المعلومات بالشكل الصحيح، وفقًا لجداول الخدمة والمواصفات الموصى بها من قبل المورد، وذلك لضمان استمرارية توفرها وسلامتها. كما يجب إعداد خطة لأعمال الصيانة الوقائية والاستباقية بهدف تعزيز توافر أنظمة المعلومات.
- يجب أن يتم تنفيذ أعمال الصيانة أو الإصلاح حصريًا من قبل أفراد صيانة مخوّلين. ويجب على شركة التجارية الاحتفاظ بقائمة بجهات الصيانة المعتمدة والأفراد المخولين العاملين لديها.
- يجب اختبار الضوابط الأمنية المطبّقة سابقًا على الجهاز أو المعدّة بعد إجراء الصيانة، وذلك للتحقق من أنها لا تزال تعمل بالشكل الصحيح. كما يجب التأكد من أن الإعدادات مطابقة لخط الأساس الأمني ويجب الاحتفاظ بسجلات مناسبة لأي أعطال مشتبه بها أو مؤكدة، بالإضافة إلى أعمال الصيانة الوقائية والتصحيحية التي تم تنفيذها.
- يجب تنظيف أجهزة تقنية المعلومات قبل إرسالها للصيانة خارج الموقع، وذلك لإزالة أي معلومات سرية قد تكون مخزنة على الأجهزة.
- يجب مراقبة وضبط أنشطة صيانة الأجهزة والمعدات سواء كانت تتم في الموقع أو خارجه.
- يجب تخزين المعدات وقطع الغيار اللازمة التي قد تُستخدم في صيانة النظام لضمان توفرها الفوري عند الحاجة.

3.30 الأمن السيبراني

- يجب المحافظة على أعلى مستويات الأمن على الشبكة وخوادم الإنتاج. ويتعين على المسؤولين عن الشبكة والاتصالات الخارجية تلقّي التدريب المناسب في تقييم المخاطر وكيفية بناء نظام آمن يقلّل من التهديدات الناتجة عن الجرائم الإلكترونية.
- يجب أن تكون الشركة مستعدة بشكل دائم، وأن تُجرى صيانة واختبارات منتظمة لضمان تقليل الأضرار الناتجة عن الهجمات الإلكترونية الخارجية المحتملة، واستعادة خدمات الأعمال ضمن الإطار الزمني المتوقع.
- الأولوية تكمن في تقليل المخاطر المرتبطة بالهجمات السيبرانية على أنظمة ومعلومات الشركة من خلال الجمع بين الضوابط التقنية والإجراءات الإدارية القوية.
- يجب الاحتفاظ بخطط الطوارئ والاستجابة لمختلف أنواع الهجمات السيبرانية، وأن تُختبر بشكل دوري لضمان كفاءتها وملاءمتها.
- تعزيز وعي الموظفين، وتشجيع اليقظة لديهم، ونشر الضوابط الوقائية والكشفية المناسبة للحد من المخاطر المرتبطة بالهجمات السيبرانية.
- لا استثناء في استخدام برامج مضادات الفيروسات المعتمدة من الشركة على جميع الأنظمة، ويجب تطبيق تحديثات تعريفات البرمجيات الخبيثة (Malware) والقيام بعمليات فحص دورية منتظمة.
- لتقليل الأثر الناتج عن إصابة البرمجيات الخبيثة، يجب تطوير إجراءات رسمية للاستجابة للحوادث المتعلقة بالبرمجيات الخبيثة، ويجب اختبارها بشكل منتظم.

3.31 الخدمات السحابية والتعاون

- تُعد منصة Microsoft 365 المنصة الرئيسية لشركة التجارية للبريد الإلكتروني والتعاون وإدارة المستندات. يجب إنشاء معلومات شركة التجارية وتخزينها ومشاركتها فقط ضمن المستأجرين والخدمات المعتمدة من الشركة؛ ويُحظر استخدام الحسابات السحابية الشخصية لمعلومات الشركة.

- يجب أن يقتصر المشاركة الخارجية عبر Microsoft 365 (مثل SharePoint وOneDrive وTeams) على الاحتياجات التجارية المشروعة، بعد الحصول على موافقة صريحة من مالك المعلومات، مع تحديد مدة زمنية عند الإمكان، ومراجعتها دوريًا. يجب تعطيل الروابط المجهولة؛ ويُسمح بالوصول فقط للمستخدمين الخارجيين المسجلين أو حسابات الضيوف.

- يجب تنفيذ حماية البريد الإلكتروني والتعاون (مثل مكافحة التصيد، الروابط والمرفقات الآمنة) والتحقق من مصداقية المرسل (SPF، DKIM، DMARC) بواسطة قسم تقنية المعلومات بالتنسيق مع أمن المعلومات.

- يجب أن تدعم قدرات الاحتفاظ، والاستكشاف الإلكتروني (eDiscovery)، والحجز القانوني في Microsoft 365 سياسة الاحتفاظ بالسجلات والقوانين المعمول بها. يظل مالكو أنظمة المعلومات مسؤولين عن تصنيف وحفظ أصول المعلومات الخاصة بهم.

- يجب أن تكون شبكات وتقنيات الموقع (مثل Wi-Fi للموقع، الكاميرات، المستشعرات، الأكشاك، الأجهزة المحمولة) معتمدة، ومقسمة عن الشبكة الأساسية، ومهيأة وفقًا لمعايير الأمان لشركة التجارية. يجب أن يكون وصول الضيوف معزولًا عن الشبكة الأساسية للشركة.

- يجب توفير وصول المقاولين من الباطن للتعاون في الموقع من خلال هويات خارجية مسجلة/حسابات ضيوف، مع الحد الأدنى من الصلاحيات، وتحديد مدة زمنية، ومراجعتها دوريًا عند الإمكان. ويجب إزالة الوصول فور انتهاء الحاجة إليه.

- يجب أن يكون استخدام الكاميرات والطائرات بدون طيار متوافقًا مع القوانين المعمول بها، وقواعد السلامة، واعتمادات شركة التجارية. يجب أن يتم تخزين ومشاركة الوسائط الملتقطة وفقًا لتصنيف الشركة وضوابط المعالجة.

4. إدارة أمن الوصول المنطقي

4.1 إدارة وصول المستخدمين

- يجب إنشاء وتنفيذ إجراءات رسمية للتحكم في منح حقوق الوصول إلى أصول المعلومات الخاصة بشركة التجارية.
- يجب تحديد متطلبات العمل للوصول إلى معلومات محددة والموافقة عليها صراحةً من قِبل مالك الخدمة المختص قبل منح المستخدمين حق الوصول إلى أصول المعلومات في الشركة.
- يجب إنشاء معرف مستخدم فريد (User ID) لكل مستخدم على الأنظمة المطلوبة، بحيث يربط الموظف بأفعاله على أنظمة المعلومات في شركة التجارية. يجب أن يتوافق معرف المستخدم مع معايير التسمية ولا يجوز أن يحتوي على أي دلالة تشير إلى حقوق وصول المستخدم، مثل كلمات "مدير" أو "مشرف" أو "متميز."
- في الحالات التي لا يكون فيها بديل لاستخدام معرفات مستخدم فريدة، يمكن مشاركة معرف مستخدم واحد بين مجموعة محددة من المستخدمين لغرض معين، ويجب أن تتم الموافقة عليه صراحةً من قِبل مدير تقنية المعلومات ومسؤول أمن المعلومات. ويجب تحميل فرد واحد المسؤولية الشخصية عن استخدام كل معرف مستخدم مشترك.
- يجب على قسم تقنية المعلومات التنسيق مع إدارة الموارد البشرية لإدارة سجلات المستخدمين الذين يحتاجون إلى الوصول إلى أنظمة المعلومات متعددة المستخدمين والخدمات وغيرها من المعدات التقنية الحيوية.
- يحدد مالكو الخدمات (أو من ينوب عنهم بشكل صريح) صلاحيات وصول المستخدمين العاديين إلى أنظمة التطبيقات، ويخولون أدوارهم بما يتناسب مع مسؤولياتهم الوظيفية.
- يجب منح وإدارة صلاحيات الوصول إلى الشبكة وخدمات الشبكة فقط بناءً على الحاجة العملية وضرورة المعرفة.(Need-to-Know)
- يجب الاحتفاظ بسجلات رسمية لجميع طلبات الوصول لإثبات موافقات الإدارة ومنح أو إلغاء حقوق الوصول.
- يتحمل مالكو الخدمات، ومدراء الأقسام، وقسم الموارد البشرية مسؤولية مشتركة في تحديث أو إلغاء صلاحيات الوصول بشكل فوري عند تغيير مهام المستخدمين أو مغادرتهم لشركة التجارية، كما يجب عليهم إجراء مراجعات دورية لإزالة معرفات المستخدمين والصلاحيات غير الضرورية أو غير الصالحة.

4.2 تسجيل الدخول الآمن

- يجب على أنظمة الشركة استخدام إجراءات تسجيل دخول آمنة كما هو مناسب، وتشمل ما يلي:
- يجب تفعيل على أجهزة الحاسوب تسلسل بدء تسجيل دخول المستخدم الآمن مثل (Ctrl + Alt + Delete) و) مفتاح ويندوز.(L +
- عند تسجيل دخول المستخدم، يجب أن تعرض الأنظمة إشعارًا قياسيًا يحذر من الدخول غير المصرح به.
- يجب ألا تُعرض كلمات المرور، أو أرقام التعريف الشخصية(PIN) ، أو المفاتيح الخاصة، أو رموز التفويض الأخرى على الشاشة، ولا يجب إرسالها عبر الشبكة بدون تشفير، أو تخزينها بدون تشفير.
- في حال إدخال بيانات اعتماد مستخدم غير صحيحة، مثل كلمات المرور، أو أرقام التعريف الشخصية(PIN) ، أو قيم الرموز(Tokens) ، أو غيرها من رموز التفويض، يجب ألا تقوم الأنظمة بالإشارة إلى أي من هذه العناصر على وجه التحديد بأنها خاطئة
- المصادقة متعددة العوامل (MFA) إلزامية للوصول عن بُعد، البريد الإلكتروني ومنصات التعاون المؤسسية، الأنشطة الإدارية ذات الامتيازات، وأي وصول من أطراف ثالثة إلى أنظمة وبيانات شركة التجارية.

4.3 إدارة الصلاحيات

- يجب التحكم في تخصيص الصلاحيات من خلال عملية تفويض رسمية، تتضمن:
- تحديد الصلاحيات المرتبطة بكل منتج نظام (مثل نظام التشغيل، ونظام إدارة قواعد البيانات) والمجموعات التي ينبغي تخصيصها لها.
- تخصيص الصلاحيات للأفراد على أساس "الضرورة للاستخدام" و"حسب الحدث" (أي الحد الأدنى المطلوب لدورهم الوظيفي فقط عند الحاجة).
- يجب أن تتبع إدارة المستخدمين ذوي الصلاحيات نفس الإجراءات المتبعة مع المستخدمين العاديين.
- يجب تنفيذ المصادقة الثنائية للأنظمة الحرجة عند الاقتضاء، ويجب أن تكون الجلسات ذات الامتياز محددة المدة عند الإمكان، مع مراقبتها وفقًا لمتطلبات التسجيل لشركة التجارية.
- تُمنح صلاحيات المسؤول المحلي فقط لموظفي قسم تقنية المعلومات المحددين لأداء مهام الدعم الفني، بعد الحصول على موافقة من مدير تقنية المعلومات ومسؤول أمن المعلومات.
- لا يجوز منح صلاحيات المسؤول المحلي للمستخدمين النهائيين غير التابعين لتقنية المعلومات إلا عند الحاجة لتطبيقات أعمال محددة، وبموافقة مدير تقنية المعلومات ومسؤول أمن المعلومات.
- يجب أن يُمنح المستخدمون حق الوصول فقط إلى الخدمات التي تم تفويضهم باستخدامها صراحةً.
- يجب التحقق من هوية المستخدمين بشكل مناسب قبل منحهم حق الوصول إلى هذه الخدمات.
- ينطبق هذا على خدمات مثل بروتوكول سطح المكتب البعيد ، وشيربوينت ، والنطاق ، والبريد الإلكتروني، والملفات والمجلدات، والشبكات اللاسلكية، والوصول عبر الويب لأجهزة الأمن، وغيرها.

4.4 إعداد وإدارة كلمات المرور

- يجب على الأنظمة التي تحتوي على معلومات مصنفة كـ "سرية" أو أعلى أن تطلب تحققًا كافيًا من هوية المستخدمين (مثل أسماء المستخدمين وكلمات المرور القوية).
- يجب اتباع إجراء رسمي لتأكيد هوية المستخدم الطالب قبل إصدار كلمة مرور جديدة أو بديلة.
- يجب أن تُطبق كلمات المرور للسماح بالوصول إلى النظام (أي لا يُسمح باستخدام كلمات مرور فارغة).
- يجب تغيير كلمات مرور حسابات البائع الافتراضية في الأنظمة والأجهزة الجديدة التي تم تنفيذها.
- يجب تخزين نسخ كلمات مرور المسؤولين بشكل آمن (بصيغة مشفرة "هاش") مع وجود نسخ احتياطية خارج الموقع لأغراض التعافي من الكوارث.
- يجب على موظفي إدارة النظام استخدام حسابات شخصية، ولا يجوز استخدام حسابات المسؤول الإداري للعمليات اليومية العادية.
- يجب تغيير كلمات المرور المؤقتة/الأولية بعد أول استخدام.
- يجب تخزين ملفات كلمات المرور بشكل مشفر.
- يجب تفعيل تعقيد كلمات المرور على جميع الأنظمة بحيث تحتوي على:
  - حرف كبير واحد على الأقل
  - حرف صغير واحد على الأقل
  - رقم واحد على الأقل
  - رمز غير أبجدي رقمي واحد على الأقل
  - يجب أن تكون كلمات المرور بطول لا يقل عن 8 أحرف.
  - يجب أن تكون كلمات المرور معقدة
- يجب ألا تكون كلمة المرور الجديدة مماثلة لأي من آخر 6 كلمات مرور تم استخدامها مسبقًا.
- يجب تغيير كلمات المرور على الأقل كل 90 يومًا.
- يجب أن يكون الحد الأدنى لعمر كلمة المرور يوم واحد.
- يجب إرسال تنبيه بانتهاء صلاحية كلمة المرور قبل 14 يومًا من تاريخ انتهاء الصلاحية.
- يجب أن تكون مدة قفل الحساب لا تقل عن 15 دقيقة.
- يجب قفل الحساب بعد 5 محاولات فاشلة لإدخال كلمة المرور.
- يجب أن يكون تسجيل الدخول مقصورًا فقط على المستخدمين الذين تم منحهم حق الوصول.
- يجب أن تكون أنظمة إدارة كلمات المرور تفاعلية وتضمن جودة كلمات المرور وفقًا للسياسة.

4.5 استخدام كلمات مرور المسؤولين

- يجب الاحتفاظ بكلمات مرور صلاحيات المسؤول الخاصة بخوادم تقنية المعلومات وأجهزة الشبكة/الأمن في ظرف مختوم داخل خزنة مقفلة أو في نظام إدارة الوصول المتميز (Privilege Access Management System).
- يجب أن تكون كلمات المرور (بما في ذلك العبارات السرية، وأرقام التعريف الشخصية) كما يلي:
  - سرية ولا تتم مشاركتها مع الآخرين (باستثناء معرفات المستخدم المشتركة/المجمعة التي تمت الموافقة عليها بشكل خاص).
  - محفوظة في الذاكرة بدلاً من كتابتها.
  - سهلة التذكر وصعبة التخمين (مثلاً، لا تحتوي على كلمات من القاموس، أو تحويرات لأسماء الشركة التجارية، أو أسماء المستخدم، أو أسماء المشاريع أو الأقسام، أو المواقع، أو تسلسلات لوحة المفاتيح البسيطة) يتم إيصالها إلى المستخدم عبر قناة مختلفة عن القناة المستخدمة لإيصال معرف الحساب.

4.6 انتهاء صلاحية الجلسة

- يجب إنهاء الجلسات غير النشطة بعد فترة زمنية محددة. فترة انتهاء الجلسة الافتراضية هي 15 دقيقة.
- أي تعديل على هذه الفترة يعتمد على تصنيف مخاطر التطبيقات، ويجب أن تتم الموافقة عليه من قبل مسؤول أمن المعلومات ومالك التطبيق المعني.

4.7 إدارة خدمة الدليل

- لإدارة الوصول إلى أصول المعلومات وحسابات المستخدمين، يجب إنشاء وإدارة دليل (Directory) كما يلي:
- يجب تصميم الدليل بطريقة تضمن أن التعديلات لا تؤثر على حقوق الوصول المعمول بها حالياً.
- يجب تعريف سياسات وصول مناسبة ضمن خدمة الدليل.
- يجب مراقبة خوادم الدليل بشكل دوري ومستمر.
- يجب أن يكون تصنيف أمان خدمة الدليل مطابقًا لأعلى تصنيف أمان للمعلومات التي تصل إليها، ويجب توثيق ذلك.
- يُسمح فقط للخوادم المعتمدة والمصادقة لها بالانضمام إلى مجموعة خدمة الدليل.
- يجب أن تتم جميع الاتصالات التي تتعلق ببيانات الاعتماد أو أذونات الوصول إلى أنظمة المعلومات باستخدام تشفير قوي.
- يجب تعيين إدارة الدليل لأشخاص مؤهلين وموثوقين فقط.
- يجب الحصول على موافقة مسؤول أمن المعلومات قبل ربط أكثر من دليل.
- لا يجوز السماح إلا للأشخاص المخولين بالوصول إلى التفاصيل الفنية لخدمة الدليل.

4.8 مراجعة حقوق وصول المستخدمين

- يجب على مسؤول أمن المعلومات التأكد من قيام مالكي الخدمات بمراجعة حقوق وصول المستخدمين بشكل رسمي مرتين في السنة، وبعد أي تغييرات جوهرية في المنظمة أو الأنظمة أو الأفراد، بالنسبة للمستخدمين على أنظمتهم المعلوماتية.
- تهدف هذه المراجعة إلى تحديد حقوق الوصول التي قد لم تعد ضرورية، وكذلك الحسابات الخاملة التي يمكن إزالتها من أنظمة المعلومات.
- يجب على مسؤول أمن المعلومات التأكد من قيام مالكي الخدمات بمراجعة حقوق الوصول المميزة (الممنوحة على أنظمة الإنتاج) سنويًا، ومقارنتها بالموافقات المسجلة لضمان عدم حصول أي صلاحيات غير مصرح بها.
- يمكن إجراء مراجعات لحقوق الوصول بشكل استثنائي في أي وقت بناءً على طلب الإدارة، مالكي الخدمات، مسؤول أمن المعلومات، أو المدققين.
- يجب مراجعة حقوق الوصول والصلاحيات، وإذا لزم الأمر إعادة الموافقة عليها من قبل المديرين عند انتقال الموظفين داخليًا، لضمان الحفاظ على صلاحيات الوصول المناسبة.
- يجب توثيق مراجعات حقوق الوصول والصلاحيات، والاحتفاظ بهذه الوثائق لمدة لا تقل عن سنة، وبصيغة مناسبة لمراجعات التدقيق.

4.9 توثيق الاتصالات الخارجية

- يجب أن يتم توثيق هوية المستخدمين الراغبين في الوصول إلى شبكات شركة التجارية عند نقطة الدخول الأولى إلى الشبكة باستخدام معرفات مستخدم فريدة وطرق توثيق مناسبة (مثل رموز الأمان التشفيرية، البطاقات الذكية مقترنة بكلمات المرور، أرقام التعريف الشخصية، و/أو المقاييس الحيوية).
- يجب تحديد أشكال الوصول عن بُعد المسموح بها.
- يجب استخدام الشبكات الخاصة الافتراضية لإنشاء والحفاظ على اتصالات الوصول عن بُعد، وعند الاتصال بالشبكة الأساسية من خلال VPN يجب تقييد الاتصال بالشبكات الأخرى.
- يجب وضع ضوابط خاصة لضمان سرية وسلامة البيانات المنقولة عبر الشبكات العامة وحماية الأنظمة المتصلة.
- يُسمح بإنشاء اتصال واحد فقط عن بُعد لكل حساب في أي وقت.
- يُمنع استخدام برامج سطح المكتب البعيد المعتمدة على الإنترنت مثل Webex إلا إذا تم التفويض من قبل إدارة أمن المعلومات. ي

- جب أن يتم الوصول عن بُعد عبر بوابات آمنة معتمدة، مع تطبيق ضوابط حالة الجهاز والوصول الشرطي عند الإمكان.

4.10 تقييد الوصول إلى المعلومات

يجب أن تتوفر في أنظمة التطبيقات العاملة عبر المنظمة آلية مناسبة للتحكم في الوصول، لضمان الحفاظ على سلامة البيانات وأمنها، ومنع أو تقييد أي وصول غير مصرح به إلى التطبيقات أو أي جزء منها.

5. أمن المعلومات في الموارد البشرية

5.1 تطبيق سياسات أمن المعلومات في الموارد البشرية

- يتولى مسؤول أمن المعلومات، وقسم إدارة المخاطر، ومالك النظام بالتنسيق مع قسم الموارد البشرية تحديد المسؤوليات المتعلقة بالحفاظ على أمن أصول ومعلومات شركة التجارية والخدمات المرتبطة بها، وذلك للمناصب الحالية في الشركة، بما يشمل المسؤوليات الخاصة بالأدوار أو الفرق التي تلعب دوراً رئيسياً في تطبيق سياسات تكنولوجيا المعلومات في التجارية .وبالتنسيق مع قسم الموارد البشرية، وقسم إدارة المخاطر، ومسؤول أمن المعلومات، يجب على كل مدير مباشر التأكد من إدراج مسؤوليات سياسات أمن المعلومات ذات الصلة ضمن توصيفات الوظائف للموظفين التابعين له.
- يجب تضمين مسؤوليات سياسات أمن المعلومات ضمن مدونة السلوك وتقديمها للمرشحين المحتملين قبل التعيين.
- يجب أن توضح مدونة السلوك التزام الموظف بالامتثال لسياسات أمن المعلومات في التجارية ، بالإضافة إلى وصف الإجراءات التأديبية التي ستُطبق في حال عدم الامتثال.
- يجب الحفاظ على فصل كافٍ للواجبات عند تعيين الأدوار والمسؤوليات المختلفة في التجارية ، كلما سمحت الظروف، وعندما تكون فوائد فصل الواجبات تفوق المخاطر التشغيلية الناتجة عن عدم وجود موظفين مدربين بديلين.
- يجب على الموظفين توقيع مدونة السلوك قبل السماح لهم بالوصول إلى أصول معلومات التجارية ، ويجب أن يحتفظ قسم الموارد البشرية بسجل رسمي يثبت قبول كل موظف.
- يُطلب من جميع الموظفين قراءة، توقيع، والالتزام بمدونة السلوك.
- يجب على كل موظف جديد حضور وإكمال دورة التوعية بأمن المعلومات خلال شهر واحد من تاريخ بدء العمل في التجارية، بالإضافة إلى إتمام جميع الدورات التدريبية الأمنية اللاحقة في مواعيدها.
- يتعين على قسم الموارد البشرية التأكد من أن جميع الموظفين على وعي كامل بمسؤولياتهم القانونية ومسؤوليات أمن المعلومات، وذلك من خلال تضمين هذه المسؤوليات في الوثائق الرئيسية للموظفين) مثل شروط وأحكام التوظيف ومدونة السلوك الخاصة بالتجارية.

5.2 فحص الموظفين والمتقدمين للوظائف

- يجب أن يخضع المتقدمون للوظائف والموظفون الحاليون الذين لم يتم فحصهم مسبقاً إلى عملية فحص من قبل الجهات المختصة وفقًا لمعايير الفحص المحددة مسبقًا، والتي تعتمد على تصنيف المخاطر الأمنية للوظيفة.
- يتولى قسم الموارد البشرية بالتعاون مع الأقسام التجارية ذات الصلة تحديد الكفاءة المطلوبة للدور الوظيفي بناءً على الخصائص والمتطلبات الخاصة بالوظيفة، وذلك وفقاً لسياسة الموارد البشرية الخاصة بشركة التجارية. ويشمل ذلك، على سبيل المثال لا الحصر: المؤهلات التعليمية، التدريب، المهارات، والخبرات.
- تُحدد الأدوار والمسؤوليات الموكلة للأفراد بناءً على مقارنة بين الكفاءة الفعلية والمتطلبات اللازمة للدور الوظيفي.
- يجب التحقق من مصداقية وصحة المؤهلات التعليمية، المؤهلات المهنية، وخلفية العمل للموظفين الجدد.

5.3 الإجراءات التأديبية

- يجب وضع إجراءات تأديبية رسمية للتعامل مع حالات عدم التزام الموظفين بسياسات أمن المعلومات. ويجب أن تتوافق هذه الإجراءات مع الأنظمة والتشريعات الحكومية ذات الصلة.
- يجب ألا تُتخذ الإجراءات التأديبية إلا بناءً على أدلة موثوقة تؤكد وقوع خرق للسياسات المتعلقة بأمن المعلومات. كما يجب أن يقتصر الاطلاع على تفاصيل هذه الإجراءات على الأطراف المعنية فقط، بناءً على مبدأ الحاجة إلى المعرفة.
- يجب استخدام نتائج الإجراءات التأديبية كمدخلات لتحسين نظام أمن المعلومات، وتفادي تكرار الحوادث المماثلة مستقبلًا.
- في حال إنهاء خدمة أحد الموظفين أو استقالته، يجب على إدارة الموارد البشرية إجراء مقابلة خروج رسمية، وإبلاغ إدارة تقنية المعلومات بذلك لضمان استرجاع كافة الأصول المسلّمة، وتنفيذ إجراءات إلغاء الوصول (سواء المادي أو المنطقي) إلى أصول وأنظمة شركة التجارية في الوقت المناسب.
- يجب على إدارة الموارد البشرية الاحتفاظ بسجل موثق لمقابلة الخروج، يتضمن جميع الأصول التي كانت بحوزة الموظف وتلك التي تم استردادها.
- يجب على شركة التجارية تحديد مدة احتفاظ مناسبة للحسابات المعطّلة أو غير النشطة، وفقًا لمتطلبات العمل والامتثال التنظيمي.
- يجب تنفيذ إجراءات إنهاء الخدمة بدقة، مع التركيز على إنهاء صلاحيات الوصول إلى الأصول والمعلومات الحساسة، بشكل فوري ومنهجي.
- في حالات الإنهاء غير الطوعي (مثل الفصل)، يجب أن تتم العملية بحضور أفراد الأمن، الذين يتولون مرافقة الموظف حتى مغادرة الموقع بعد جمع متعلقاته الشخصية، بما يتوافق مع السياسات الأمنية للشركة.

6. إدارة حوادث أمن المعلومات

6.1 الإبلاغ عن الحوادث والأحداث الأمنية

يجب على موظفي شركة التجارية الإبلاغ عن أحداث أمن المعلومات إلى مكتب خدمة تقنية المعلومات في أقرب وقت ممكن بعد وقوعها.يجب إنشاء آليات مخصصة للإبلاغ عن هذه الحوادث، تشمل على سبيل المثال لا الحصر :بوابة مكتب ،قنوات الهاتف ،قنوات البريد الإلكتروني تشمل أحداث أمن المعلومات، على سبيل المثال لا الحصر:

- انتهاك أو عدم الامتثال لسياسات تقنية المعلومات الخاصة بشركة التجارية، أو لأي قوانين أو لوائح أخرى ذات صلة بالمخاطر، والرقابة، والحوكمة الخاصة بتقنية المعلومات وخدمات الشركة.
- سلوك غير طبيعي في أنظمة تقنية المعلومات، مثل الأعطال، أو الأخطاء البرمجية، أو رسائل الخطأ، أو الفيروسات، أو التنبيهات والإنذارات، أو التأخيرات، أو النتائج غير المتوقعة.
- فقدان خدمات أو معدات أو مرافق تقنية المعلومات، بما في ذلك السرقة، أو التلف، أو الأعطال، أو التحميل الزائد، أو الحوادث، أو الأخطاء البشرية، أو أي ظروف تؤدي إلى انقطاع الخدمة.
- هجمات التصيّد الإلكتروني .
- تغييرات غير مصرح بها أو غير مضبوطة على الأنظمة.
- اكتشاف صلاحيات وصول غير مناسبة.
- سوء استخدام الأنظمة.
- فشل في الحفاظ على سرية المعلومات (مثل الوصول غير المصرح به إلى المعلومات الحساسة أو الإفصاح عنها).
- انتهاك سياسات الوصول إلى الشبكات أو الأنظمة أو البيانات.
- بعد التحقق الأولي من الحدث المُبلغ عنه، يقوم مكتب خدمة تقنية المعلومات بإبلاغ قسم أمن المعلومات.
- وسيبدأ قسم أمن المعلومات (ISS) بتفعيل إجراءات الاستجابة المناسبة للحادث، وذلك وفقًا لـ إطار عمل الاستجابة للحوادث المعتمد لدى الشركة.

6.2 الإبلاغ عن مواطن الضعف الأمنية

يُمنع على الموظفين محاولة استكشاف أو تقييم أو تأكيد أو إثبات وجود مواطن ضعف أمنية مشتبه بها بأنفسهم، وذلك في الحالات التي قد تؤدي إلى:

أ- حدوث خروقات أمنية جسيمة،
ب- التأثير على عمليات التحليل الجنائي الرقمي(Forensic Analysis) ، أو
ت- اعتبار هذا التصرف إساءة استخدام متعمدة للنظام، مما قد يؤدي إلى إجراءات تأديبية أو قانونية.

- وبالمثل، لا يجوز للموظفين محاولة إصلاح الأعطال البرمجية أو التعامل معها إلا إذا تلقوا تعليمات صريحة من مكتب خدمة تقنية المعلومات للقيام بذلك

6.3 تخطيط إدارة حوادث أمن المعلومات

- يجب أن يتضمن التخطيط الخاص بإدارة حوادث أمن المعلومات من قبل فريق أمن المعلومات – إدارة المخاطر ما يلي:
- يجب أن يستند خطة إدارة أمن المعلومات إلى بيانات الحوادث المتوقعة، وأن تتم مراجعتها من قبل إدارة المخاطر.
- يجب إعداد قوائم مرجعية (Checklists) تُحدد الأنشطة التي يتعيّن تنفيذها لاحتواء الحوادث المتوقعة، بما في ذلك الالتزامات المتعلقة بالإبلاغ إلى الجهات المعنية داخليًا وخارجيًا والمتأثرة بالحوادث.

- يُسمح فقط للأشخاص المخولين رسميًا بالوصول إلى إطار إدارة الحوادث والأدوات الداعمة له.
- يجب تطوير قاعدة معرفة مركزية تحتوي على تفاصيل الحوادث المُحددة مسبقًا، والحلول المقابلة لها.
- يجب إعداد مصفوفة تشخيص (Diagnosis Matrix) لمساعدة فريق تقنية المعلومات في التعرّف السريع على نوع الحادث واتخاذ الإجراءات التصحيحية المناسبة.

- يجب الحفاظ على علاقات تعاون مستمرة مع الجهات الخارجية المزوّدة لخدمات حماية نظم المعلومات، وذلك للبقاء على اطلاع دائم بأحدث الحوادث الأمنية وطرق الاستجابة المحتملة لها.
- في حال وجود حوادث جسيمة محتملة، يجب الحصول على موافقة مسبقة من الإدارة لفريق أمن المعلومات – إدارة المخاطر ، ويجب أن تكون هذه الإجراءات متفق عليها من قِبل أصحاب المصلحة الرئيسيين لاتخاذ الإجراء المناسب.

6.4 المسؤوليات والإجراءات

إدارة الحوادث يجب أن تتم بواسطة فريق إدارة أمن المعلومات – إدارة المخاطر تكون أدوارهم ومسؤولياتهم واضحة ومحددة. يجب أن تضمن مسؤوليات وإجراءات إدارة الحوادث استجابة سريعة وفعالة ومنظمة لحوادث أمن المعلومات. كما يجب دمج مراقبة أنظمة المعلومات وتسجيل الأحداث مع أنشطة إدارة الحوادث.

- إجراءات الاستجابة للحوادث يجب أن تشمل:
  - تصنيف وتبويب الحوادث بناءً على خطورتها وتأثيرها.
  - تحليل الأحداث الأمنية المبلغ عنها والثغرات، ومراقبة الأنظمة والتنبيهات، لتحديد وترتيب أولويات الأحداث الأمنية التي تشير إلى حدوث حوادث فعلية أو محتملة في حال عدم منعها.
  - احتواء الحوادث (مثل فصل الأنظمة المتأثرة عن الشبكة لحين إجراء المزيد من التحليل).
  - تحليل وتحديد أسباب الحوادث (ما الذي حدث بالضبط؟ من هم الأطراف أو الأصول التقنية المتورطة؟ ما الضوابط التي كانت مفقودة أو فشلت؟ ما الأضرار التي لحقت بالشركة؟).
  - تطبيق الدروس المستفادة من الحوادث لتحقيق تحسين مستمر في قدرة شركة "التجارية" على إدارة مخاطر أمن المعلومات.
  - الاحتفاظ بسجلات النظام، ومسارات التدقيق، والأدلة الجنائية المماثلة.

يجب مراجعة ومتابعة الحوادث الأمنية الكبرى وفقاً لإطار عمل الاستجابة للحوادث.

6.5 تدريب ومحاكاة حوادث أمن المعلومات

- يجب تدريب الأفراد المكلفين على احتواء الحوادث من خلال محاكاة سيناريوهات الحوادث.
- يجب أن يقوم منسق بتطوير محاكاة الحوادث، ويُحتفظ بسجل بنتائج التدريب. ويجب استخدام النتائج المستخلصة من المحاكاة والتدريب لتحسين إطار عمل إدارة الحوادث.
- يجب تبديل أعضاء فريق إدارة أمن المعلومات – إدارة المخاطر (قسم البنية التحتية لتقنية المعلومات والعمليات) دون إشعار مسبق، بهدف اختبار كيفية إدارة الحوادث في حال غياب الأدوار الرئيسية.
- يجب إجراء تدريبات منتظمة (على الأقل سنويًا) لضمان تحديث فريق إدارة الحوادث بأحدث الاتجاهات والممارسات في إدارة حوادث أمن المعلومات

6.6 إدارة استجابات حوادث الأمن

- يجب السماح لفريق إدارة أمن المعلومات – إدارة المخاطر بإجراء تحقيق مستقل في الحوادث. وفي حالة الحوادث الكبرى، يتم تعيين منسق حادث واحد ليتمكن من إدارة الحادث بسلطة كاملة.
- يجب إنشاء واستخدام أدوات دعم وقوائم مراجعة لإدارة الحوادث بشكل فعال.
- يمكن لضابط أمن المعلومات أو مدير تقنية المعلومات إجراء تحقيق مستقل بدعم من أطراف ثالثة.

6.7 إدارة الأدلة الأمنية

- يجب تطوير واتباع إجراء محدد للحالات التي يتم فيها تصعيد الحادث إلى مستوى يتطلب اتخاذ إجراء قانوني. يجب جمع الأدلة الكافية والاحتفاظ بها بما يتوافق مع القوانين والأنظمة ذات الصلة.
- تتكون إدارة الأدلة من أربع مراحل: جمع البيانات، الفحص، التحليل، والتقرير.
- يجب أن يكون فريق إدارة أمن المعلومات – إدارة المخاطر (ISS – Risk Management) مؤهلاً لإدارة الأدلة.
- يجب تخزين الأدلة في مكان آمن مع سياسات تحكم وصول محددة بشكل واضح.
- يجب الاحتفاظ بسجلات (Logs) تتعلق بالإجراءات التي تُجرى على الأدلة.
- يمكن إشراك جهات خارجية (محامون أو الشرطة) إذا تطلب الأمر للتحقيق.
- يجب الحصول على الأدلة الرقمية بوسائل تحميها من الكتابة أو التعديل(write-protected) .

6.8 التحليل بعد الحوادث، التقرير، والإجراءات التصحيحية

- يجب أن يشارك كل من فريق إدارة أمن المعلومات – إدارة المخاطر والأطراف المتأثرة في مراجعة الحادث بعد وقوعه. ويجب إعداد تقرير يتضمن النتائج الهامة التي تم التوصل إليها عقب المراجعة.
- يجب أن يُعتمد هذا التقرير من قبل وحدة إدارة المخاطر، حيث تُحدد الإجراءات التصحيحية المناسبة لاحتواء الحوادث.
- يجب قياس ومراقبة أنواع وأحجام وتكاليف الحوادث الأمنية (عند الاقتضاء) لتحديد الحوادث أو الأعطال المتكررة أو ذات التأثير الكبير، مما يشير إلى الحاجة لتعزيز أو إضافة ضوابط وتحديث سياسات تقنية المعلومات في شركة "التجارية."
- مع مراعاة السرية (مثل إزالة تفاصيل الأفراد المعنيين أو المعلومات الحساسة الأخرى)، يمكن استخدام حوادث أمن المعلومات لأغراض التوعية الأمنية.

7. إدارة الأصول

7.1 جرد الأصول

يجب تسجيل ومراجعة وصيانة وتدقيق جرد أصول الشركة على أساس دوري.

7.2 تصنيف أصول المعلومات

- يجب تصنيف المعلومات التي بحوزة شركة "التجارية" إلى فئات: عامة، داخلية، سرية، أو سرية جدًا، بناءً على حساسية كل منها.
- التصنيف الافتراضي للأصول يكون "سرية" حتى يتم تعيين تصنيف محدد لها.
- يجب أن يتوافق تصنيف نظام المعلومات مع أعلى تصنيف للبيانات الموجودة عليه أو التي تمر من خلاله.
- يجب مراجعة تصنيف أصول المعلومات بانتظام من قِبل مالكي الخدمة المسؤولين عن هذه الأصول، وبالتنسيق مع مسؤول أمن المعلومات وقسم إدارة المخاطر.
- يجب إجراء تحليل تأثير عند الحاجة إلى إعادة تصنيف أصل معلومات، ويجب إبلاغ أصحاب المصلحة المعنيين بعملية إعادة التصنيف.

7.3 الاحتفاظ بالمعلومات والتخلص منها

- تُعد إدارة الملفات والبيانات بشكل فعّال أمرًا حيويًا لتمكين شركة "التجارية" من أداء وظائفها التشغيلية. توفر سياسة الاحتفاظ والتخلص من البيانات إرشادات واضحة بشأن الاحتفاظ والتخلص من بيانات الشركة، وتضمن ما يلي:
  - **أ-** إمكانية استرجاع البيانات وتتبعها بسهولة.
  - **ب-** الاحتفاظ بها فقط للفترة اللازمة.
  - **ت-** التخلص منها بطريقة مناسبة لمنع وقوعها في أيدي أشخاص غير مخولين.
  - **ث-** تخزينها بشكل ملائم مع مراعاة حساسية وسرية المواد المسجلة.
- يتحمل كل مالك لأصول المعلومات مسؤولية النظر في الأمن عند استخدام المعلومات أو التخلص منها في جميع الظروف. وتكون الأقسام أو الوحدات أو الموردين الذين يُعتبرون مالكي أو أمناء معلومات رئيسيين مسؤولين عن تحديد وتوثيق فترة الاحتفاظ بالمعلومات الحيوية.
- تقوم شركة "التجارية" بتحديد فترات الاحتفاظ المناسبة لأنواع معينة من المعلومات كما هو منصوص عليه من وقت لآخر بواسطة الجهات التنظيمية والإرشادات المعمول بها. ويجب على كل قسم أو وحدة أو مورد وضع إجراءات مناسبة للمعلومات التي يحتفظون بها ويعالجونها، وضمان إطلاع جميع الأطراف ذات الصلة على هذه الإجراءات.
- يجب على الأقسام أو الوحدات أو الموردين الاحتفاظ بالسجلات والمعلومات إذا:
- من المحتمل الحاجة إليها في المستقبل، ما لم تكن هناك دورة احتفاظ محددة منصوص عليها في سياسة معينة لضمان توفرها في الوقت المناسب.
  - **أ-** يتطلب التنظيم أو القانون الاحتفاظ بها.
  - **ب-** من المحتمل الحاجة إليها للتحقيق أو الملاحقة في حالات الأفعال غير المصرح بها أو غير القانونية أو المسيئة، أو لتمكين شركة "التجارية" من الاستجابة لطلبات الكشف، أو الاستدعاءات القانونية، أو مطالبات التحقيق، أو غيرها من الطلبات المتعلقة بالإجراءات القانونية أو التنظيمية.
- يجب التخلص من المعلومات الحساسة وفقًا لإجراءات التخلص الخاصة بتصنيفات المعلومات المختلفة، لضمان إزالة كاملة وآمنة للمعلومات المصنفة كـ "سرية جدًا"، "سرية"، أو "داخلية"، سواء كانت في شكل ورقي أو إلكتروني. تشمل إجراءات التخلص التمزيق، التنسيق منخفض المستوى، إزالة التمغنط لأقراص التخزين الصلبة، وغيرها.
- سيُعرض من يقوم بالتدمير أو التخلص غير المصرح به لمعلومات الشركة الحساسة لإجراءات تأديبية، بما في ذلك الفصل والملاحقة القانونية.

7.4 إدارة الوسائط القابلة للإزالة

- يجب على قسم تقنية المعلومات تطوير وتوثيق وتنفيذ إجراءات لإدارة الوسائط القابلة للإزالة.

8. إدارة الموردين من الأطراف الثالثة

8.1 تحديد متطلبات الموردين من الأطراف الثالثة

- يجب تحديد أنواع الأطراف الخارجية والمخاطر المتعلقة بأمن المعلومات المرتبطة بها وتوثيقها. وبعد ذلك، يجب تحديد متطلبات الأمن السيبراني اللازمة لمعالجة هذه المخاطر.
- يجب تضمين متطلبات أمن المعلومات في طلبات العروض (RFP) وطلبات التسعير .(RFQ) كما يجب إلزام المورد من الطرف الثالث بإدراج التزامه بمتطلبات أمن المعلومات الخاصة بالشركة في ردوده على طلبات العروض و/أو التسعير، والتي تُنقل لاحقًا إلى الاتفاقية في حال تم منح العقد للمورد.
- في حال عدم الالتزام بمستويات الخدمة المتفق عليها من قبل الموردين من الأطراف الثالثة، يجب تصنيف ذلك كمخاطرة، وتسجيلها في سجل المخاطر، ووضع خطة للتخفيف من تلك المخاطر.

8.2 اختيار الموردين مع التركيز على الأمان

- يجب إلزام الموردين من الأطراف الثالثة بتوقيع اتفاقية عدم إفشاء (NDA) قبل مشاركة أي معلومات حول الوضع الحالي لأمن المعلومات واحتياجات الشركة المستقبلية ضمن طلبات العروض (RFPs) وطلبات التسعير.(RFQs)
- يجب مراجعة وتقييم مقترحات الموردين بناءً على مدى تلبية المورد من الطرف الثالث لمتطلبات أمن المعلومات المحددة في طلبات العروض وطلبات التسعير. ولا يجوز منح العقد للموردين الذين لا يستوفون الحد الأدنى من متطلبات أمن المعلومات أو الذين يُكتشف لديهم مشكلات أمنية أخرى.
- لأغراض تعهيد استضافة مراكز البيانات، يمكن استضافة معلومات الشركة المصنفة ضمن مستوى "سرية" أو أعلى خارج دولة الكويت.
- يجب إجراء مناقشات ومراجعات وتفتيشات/تدقيقات للموردين المحتملين عند الضرورة، لتقييم مدى قدرتهم على تلبية متطلبات الأمن والحفاظ عليها قبل إبرام العقود.

8.3 إدارة اتفاقيات موردي الطرف الثالث

يجب مراعاة الأمور التالية عند تضمين متطلبات أمن المعلومات في اتفاقية مع مورد طرف ثالث (عند الاقتضاء):

- المخاطر المرتبطة بنوع المورد وتأثيرها على الأمن العام لشركة "التجارية"، بما في ذلك المتطلبات القانونية والتعاقدية.
- التزامات المورد تجاه نشر الوعي وضمان الامتثال لسياسات تقنية المعلومات الخاصة بـ "التجارية" بين العاملين الذين يرسلهم المورد.
- متطلبات الوصول المنطقي للمستخدمين والمديرين.
- متطلبات الوصول المنطقي للاتصالات الخارجية بشبكة "التجارية"، والتي تتطلب تفاصيل عن الشخص المعتمد للموافقة على الربط، والأنظمة المشاركة، ومسارات الاتصال المستخدمة، وحماية المعلومات المتبادلة.
- حساسية المعلومات التي سيصل إليها المورد (يجب تحديد متطلبات الامتثال لمعايير تصنيف ومعالجة المعلومات الخاصة بـ "التجارية" حسب نوع التصنيف وإدراجها في العقد).
- المستوى المستهدف للخدمة والأمن، بالإضافة إلى مراقبة أداء المورد مقابل متطلبات الأمن التعاقدية والامتثال ضمن فترات مخططة محددة.
- عملية إدارة التغيير التي سيتبعها المورد.
- متطلبات الوصول الفيزيائي.
- تأثير الاتفاقية على متطلبات استمرارية الخدمة.
- متطلبات ضمان الهوية والمصادقة متعددة العوامل (MFA) لأي وصول منطقي إلى أنظمة الشركة أو بياناتها، بما في ذلك التعاون مع الضيوف/الأطراف الخارجية عبر Microsoft 365.
- التزامات على المقاولين والأطراف الثالثة بالامتثال لمتطلبات شركة التجارية الخاصة بالاستخدام المقبول للذكاء الاصطناعي، مع حظر رفع بيانات الشركة السرية/بيانات العملاء/البيانات الشخصية إلى أدوات الذكاء الاصطناعي الخارجية دون موافقة خطية مسبقة من الشركة.
- متطلبات التسجيل والمراقبة لوصول الأطراف الثالثة، بما في ذلك الاحتفاظ بالسجلات وحق تدقيقها فيما يتعلق بخدمات الشركة.
- يجب أن ينص العقد مع المورد الخارجي على العقوبات أو الإجراءات التي يمكن فرضها على المورد في حال عدم امتثاله لمتطلبات أمن المعلومات المنصوص عليها في العقد.
- يجب أن ينص العقد على التزام المورد الخارجي بالإفصاح عن أي مخاطر محتملة قد تنشأ من تنفيذ أنشطة مختلفة على أصل المعلومات محل التركيز.
- يجب أن تتضمن اتفاقيات تقديم الخدمة مع الموردين الخارجيين ضوابط أمنية وتعريفات للخدمات ومستويات للتسليم، على أن يتم تنفيذها وتشغيلها وصيانتها من قبل المورد الخارجي.
- يجب أن تتضمن عقود الموردين الخارجيين بند "حق التدقيق" بما يمنح شركة التجارية صلاحية فحص وتقييم العمليات الداخلية للموردين الخارجيين ذات الصلة بالعقد، بما في ذلك السياسات والإجراءات الأمنية الموثقة، وضوابط التغيير، ومسارات التدقيق، والعمليات الخاصة بتحديد وإدارة وحل والإبلاغ عن الحوادث الأمنية.

8.4 إدارة وصول موردي الطرف الثالث

- يجب تقييد وصول موردي الأطراف الثالثة إلى أصول معلومات "التجارية" ليشمل فقط الجهات والأشخاص المخولين. ويجب أن يكون الوصول عن بُعد أو في الموقع لأطراف خارجية إلى شبكة أو أنظمة "التجارية" مستندًا إلى المتطلبات التالية:
- يجب على مالكي الخدمات منح إذن مسبق صريح لوصول موردي الأطراف الثالثة عن بُعد إلى أصولهم. وإذا لم يكن بالإمكان منح وصول مباشر للمورد، يجب على مالك الخدمة تعيين أحد موظفي "التجارية" للإشراف على موظفي الطرف الثالث.
- يجب مراجعة قائمة الوصول المنطقي المخول لموردي الطرف الثالث، والتي يحتفظ بها قسم تقنية المعلومات، كل ستة أشهر، وعند طلب مسؤول أمن المعلومات، لتأكيد استمرار الحاجة لهذا الوصول.
- يجب الاحتفاظ بسجلات (Logs) لجميع الاتصالات عن بُعد المستخدمة من قبل موردي الأطراف الثالثة ومراجعتها بشكل أسبوعي.
- يجب إعادة تكوين أو إزالة الوصول عن بُعد الممنوح لموردي الأطراف الثالثة فور انتهاء العلاقة التعاقدية معهم، أو انتهاء مدة العقد/الاتفاقية، أو إذا قرر مالك الخدمة أو مسؤول أمن المعلومات إنهاء الترتيب لأي سبب آخر.
- يجب أن تحتفظ إدارة الخدمات العامة، بالتعاون مع قسم تقنية المعلومات وقسم الإدارة - الخدمات العامة (المسؤولين عن موردي الطرف الثالث)، بقائمة الوصول الفيزيائي لموردي الطرف الثالث في الموقع، ومراجعتها كل ستة أشهر.
- يجب أن يتم التعاون الخارجي عبر Microsoft 365 باستخدام هويات ضيوف/خارجية مسماة ومخصصة للجهات المتعاقدة. ويجب أن يكون الوصول وفق مبدأ الحد الأدنى من الصلاحيات، ومحدد المدة عند الإمكان، ويتم مراجعته بشكل ربع سنوي على الأقل من قبل مالك المعلومات، مع إلغائه فورًا عند انتهاء العقد أو تغيير الأفراد.

8.5 تقديم خدمات الطرف الثالث

- يجب إجراء فحوصات خلفية أمنية على موظفي الطرف الثالث الذين يتعاملون مع أصول أو أنظمة معلومات "التجارية". يمكن لشركة "التجارية" القيام بهذه الفحوصات بنفسها، أو طلب أدلة مناسبة من موردي الطرف الثالث تثبت صلاحية هؤلاء الموظفين.
- يجب على موردي الطرف الثالث تقديم تقارير دورية تصف فعالية وحالة ضوابط الأمن المطبقة لحماية أصول معلومات "التجارية"، ومشاركتها مع "التجارية" عند الاقتضاء .يجب التحقق من صحة وسلامة بيانات المراقبة المستلمة من موردي الطرف الثالث لضمان مصداقيتها وسلامتها.

8.6 مراقبة ومراجعة خدمات الطرف الثالث

- يجب مراجعة الخدمات والتقارير والسجلات المقدمة من مورد الطرف الثالث، كما يجب إجراء عمليات تدقيق عند الضرورة وبشكل منتظم.
- يجب مراقبة الخدمات المقدمة من موردي الطرف الثالث للتأكد من أنها تُقدم وتُدار بما يتوافق مع متطلبات أمن المعلومات الحالية، ومتطلبات العمل، والالتزامات التعاقدية، وذلك بوتيرة تتناسب مع مدة العقد ونوع الخدمة المقدمة.
- يجب قياس أداء مورد الطرف الثالث مقابل الأهداف المتفق عليها للخدمة وغيرها من الالتزامات التعاقدية.
- يجب إجراء مراجعة سنوية على الأقل لقدرات أمن المعلومات لدى موردي الخدمات المتعاقد عليهم، وذلك لضمان أن قدراتهم في حماية معلومات "التجارية" لا تزال مناسبة، ولاستمرار توافق أهداف التعاقد مع متطلبات أمن المعلومات.
- يجب تعيين أدوار أو فرق محددة تكون مسؤولة عن إدارة العقود والعلاقات مع الموردين.
- يجب منح العقد فقط لمورد طرف ثالث إذا كانت قدراته في أمن المعلومات تتماشى مع متطلبات شركة "التجارية". كما يجب إنهاء العقد في حال تكرار انتهاك متطلبات أمن المعلومات المتفق عليها.

8.7 إدارة التغييرات في خدمات الطرف الثالث

- يجب إدارة ومراقبة التغييرات المتعلقة بتقديم الخدمات، بما في ذلك صيانة وتحسين سياسات وإجراءات وضوابط تقنية المعلومات القائمة، وفقًا لإجراءات إدارة التغيير المعتمدة لدى "التجارية"، مع الأخذ بعين الاعتبار تصنيف الخدمة المدعومة وتصنيف أنظمة المعلومات والعمليات ذات الصلة.
- يجب أن تخضع التغييرات في عقود موردي الطرف الثالث لعملية إدارة التغيير لدى "التجارية".

9. حماية البيانات والخصوصية

- يتعين على الإدارة القانونية تحديد جميع القوانين واللوائح ذات الصلة المتعلقة بخصوصية البيانات وحماية المعلومات الشخصية، ويتحمل قسم أمن المعلومات مسؤولية الالتزام بهذه القوانين واللوائح المحددة.
- يقوم قسم أمن المعلومات بتحديد الضوابط اللازمة لحماية معلومات العملاء من الاستخدام أو الإفصاح أو الإتلاف أو التعديل غير المصرح به، وذلك بما يتماشى مع الأنظمة واللوائح المعمول بها.
- يجب على المستخدمين الحصول على موافقة قسم أمن المعلومات قبل جمع أو معالجة أو تخزين أو الكشف عن المعلومات السرية أو معلومات العملاء.
- يجب التعامل مع بيانات الموظفين والعملاء على أنها سرية للغاية، ولا يجوز الاطلاع عليها إلا من قبل الأشخاص المفوضين رسميًا.
- يُثني الموظفون عن مشاركة تفاصيل رواتبهم الشخصية أو شروط العمل الأخرى مع زملائهم.
- يجب على جميع المستخدمين اعتبار كلمات المرور معلومات خاصة وسرية للغاية. ويُعد عدم الامتثال لهذه السياسة سببًا قد يؤدي إلى اتخاذ إجراءات تأديبية.

9.1 المراسلات الإلكترونية

يجب حماية المعلومات المتداولة عبر وسائل المراسلات الإلكترونية مثل الإنترنت والبريد الإلكتروني والفاكس من سوء الاستخدام، أو الوصول غير المصرح به، أو التعديل، أو حجب الخدمة.

9.2 حماية بيانات الاختبار

يجب اختيار بيانات الاختبار بعناية، وحمايتها، والتحكم فيها لتجنب استخدام المعلومات التشغيلية أو أي معلومات سرية أخرى.

9.3 الخصوصية وحماية المعلومات الشخصية القابلة للتحديد

يجب الالتزام بسياسة الخصوصية الخاصة بشركة "التجارية" فيما يتعلق بحماية خصوصية المعلومات الشخصية القابلة للتحديد، بالإضافة إلى البنود التعاقدية ذات الصلة، والتشريعات المحلية والدولية المعمول بها.

9.4 الذكاء الاصطناعي والبيانات الشخصية

يحظر رفع أو كشف بيانات شركة التجارية السرية إلى أدوات الذكاء الاصطناعي الخارجية/العامة، ما لم تتم الموافقة الصريحة من ادارة الشركة.

10. التصميم والتطوير والاختبار الآمن للخدمات

10.1 تصميم وتطوير نظم المعلومات

- يجب تنفيذ تصميم وتخطيط نظم المعلومات بما يشمل تعريف متطلبات أمن المعلومات بشكل واضح قبل اختيار أو تطوير أو نشر أو تنفيذ أي خدمات جديدة أو إدخال تغييرات جوهرية على الخدمات الحالية. ويجب أخذ أمن المعلومات في الحسبان في المراحل المبكرة من دورة حياة تطوير الأنظمة، بما في ذلك دراسات الجدوى، مقترحات الميزانية، طلبات العمل، وغيرها من مستندات المبادرة والتخطيط.
- بعد الموافقة على مشاريع تطوير الأنظمة أو تغييرها، يكون مديرو المشاريع، بالتعاون مع مسؤول أمن المعلومات، مسؤولين عن الالتزام بدورة حياة تطوير البرمجيات وطرق التوريد المعتمدة لدى "التجارية."
- يجب تحديد متطلبات الأمان الخاصة بالخدمة الجديدة أو التعديلات على الخدمة الحالية بشكل رسمي في بداية المشروع. ويجب الحصول على مدخلات مسؤول أمن المعلومات لضمان توثيق المتطلبات الأمنية بشكل مناسب، مع التأكد من توافقها مع المتطلبات التشغيلية لنظام المعلومات.
- يجب إعداد وثيقة تصميم للنظام توضح الضوابط الأمنية التي سيتم تنفيذها لتلبية متطلبات الأمان المحددة. ويجب أن تتم الموافقة على التصميم من قبل مالك الخدمة وقسم أمن المعلومات قبل البدء في تطوير الخدمة.
- يجب اختيار الضوابط الأمنية وتطبيقها عبر مستويات متعددة من النظام، مثل واجهة المستخدم، طبقة التطبيق الخلفية، وطبقة قاعدة البيانات.
- في حال الضرورة، يجب إجراء تقييم مبدئي عالي المستوى للمخاطر الأمنية، على أن يُستكمل بتحليل مفصل لتوضيح متطلبات الضوابط الأمنية، بما يعكس قيمة أصول المعلومات والتأثير المحتمل للحوادث الأمنية.
- يجب التشاور مع مالكي الخدمات المعنيين ومسؤول أمن المعلومات خلال مراحل تصميم وتطوير النظام الجديد أو التعديلات الكبيرة لضمان فعالية النظام المقترح في تلبية المتطلبات التشغيلية إلى جانب الضوابط الأمنية المطبقة.
- يجب أن تتضمن خطط تنفيذ الأنظمة الجديدة أو تلك التي خضعت لتغييرات جوهرية تحديد متطلبات السعة والتوافر في البنية التحتية لتقنية المعلومات، بالإضافة إلى إجراءات استرجاع البيانات بعد الخطأ وخطط الطوارئ.

10.2 اختبار وتنفيذ نظم المعلومات

- يجب اختبار نظم المعلومات قبل تنفيذها.
- يجب إعداد خطة اختبار تتضمن حالات اختبار لتقييم فعالية ضوابط الخدمة/النظام مقابل متطلبات الأمان المحددة. ويجب تعديل أي جوانب تفشل في اختبار الأمان لتحقيق التوافق. كما يجب اختبار الأنظمة لمواجهة الهجمات الخبيثة المحتملة. يجب إجراء اختبارات الأمان وفقاً لإجراءات دورة حياة تطوير النظام والاختبار المعتمدة من قبل التجارية.
- يجب توثيق نتائج اختبارات الأمان ضمن تقرير اختبار. وإذا فشل أحد الضوابط في الاختبار، يجب تسجيل ذلك في التقرير مع محاولات الاختبار اللاحقة. وإذا تعذر تعديل الضابط الذي فشل في الاختبار، فيجب تطبيق ضابط تعويضي وتوثيقه ضمن التقرير. يجب معالجة الثغرات الأمنية المعروفة/المتأصلة في نظم المعلومات من خلال ضوابط تعويضية مناسبة يتم تحديدها من قبل مالك الخدمة، بناءً على توصية مسؤول أمن المعلومات.
- عند إتمام اختبار الأمان بنجاح، يجب أن يوقع مالك الخدمة على تقرير الاختبار لإثبات أن نظام المعلومات المختبر متوافق مع متطلبات الأمان، ولا يحتوي على وظائف غير ضرورية مفعلة، وذلك قبل نقله إلى بيئة الإنتاج.
- يجب تأمين بيانات الاختبار وفقاً لتصنيف البيانات. ولا يجوز استخدام بيانات الإنتاج في التطوير أو الاختبار ما لم يتم نزع حساسية البيانات أو تشفيرها. كما يجب إخضاع أنظمة الاختبار لنفس ضوابط الوصول المطبقة على أنظمة الإنتاج المناظرة.
- يجب تطبيق الإعدادات (التكوينات) على نظم المعلومات وأجهزة الشبكة وفقاً لأسس التشديد الأمني، وباستخدام إرشادات أمن المعلومات ومعايير الأمن المعتمدة لدى التجارية، وذلك قبل نشرها في بيئة الإنتاج.
- لا يجوز نقل أي نظام معلومات إلى بيئة الإنتاج ما لم تتم إزالة جميع حسابات المسؤولين وحسابات الاختبار والتطوير منه. كما يجب إزالة بيانات الاختبار من النظام بعد الانتهاء من الاختبار.
- يجب منح صلاحيات الوصول إلى نظم المعلومات وفقاً لما ورد في سياسة "إدارة أمن الوصول المنطقي."
- يجب مراجعة البرمجيات الجديدة وأي أجزاء جديدة من الشيفرة المصدرية في البرمجيات القائمة) مثل استعلامات وإجراءات (SQL لضمان الجودة قبل النشر، كلما أمكن ذلك.
- عند تنفيذ نظام معلومات جديد أو عند حدوث تغيير جوهري في النظام القائم، يجب مراعاة ما يلي:
- يجب توفير دليل تشغيل يغطي إجراءات بدء التشغيل، الإيقاف، واستعادة الخدمة، وذلك قبل إدخال النظام الجديد.
- يجب توفير الأدلة التشغيلية والتدريب المناسب للمستخدمين النهائيين، حسب الحاجة، قبل استخدام نظام المعلومات
- يجب إجراء نسخ احتياطي للأنظمة والبيانات بشكل منتظم، كما يجب اتخاذ ترتيبات مناسبة لضمان القدرة على الصمود واستعادة الأعمال في حالات الكوارث.

- يجب على قسم البنية التحتية لتقنية المعلومات والعمليات تنفيذ اختبارات أمنية بشكل ربع سنوي، وتشمل - على سبيل المثال لا الحصر - ما يلي:

أ- فحص الثغرات الأمنية باستخدام بيانات اعتماد (فحص مصادق عليه).

ب- فحص التوافق مع معيار أمن المعلومات المعتمد لدى التجارية.

ت- مراجعة إعدادات التكوين.(Configuration Review) .

10.3 التحكم في البرمجيات التشغيلية

- يجب الاحتفاظ بتفاصيل عن البرمجيات المعتمدة والمدعومة، بما في ذلك المعلومات المتعلقة بالبرمجيات التي سبق اعتمادها.
- يجب استخدام برمجيات الأمان فقط من قبل الأشخاص المخوّلين وللأغراض المصرح بها.
- يجب أن يتم التحكم في تنفيذ البرمجيات على أنظمة الإنتاج للحد من مخاطر تلف الأنظمة التشغيلية. ولا يُسمح إلا للأشخاص المعينين بتنفيذ تحديثات مكتبات البرامج في بيئة الإنتاج، ويجب أن تكون هذه التحديثات مصرح بها ومُسجّلة.
- يجب أن تمنع ضوابط نظام التشغيل استخدام أي برمجيات غير مصرح بها قد تتجاوز ضوابط أمن المعلومات أو تتيح وصولًا مباشرًا إلى برامج التطبيقات وملفات البيانات (بما في ذلك أدوات/برامج التطبيقات، ملفات الإعداد/المعلمات، سكربتات بدء/إيقاف التطبيقات، وملفات سجلات التطبيقات) من قبل مستخدمين آخرين.
- يجب الاحتفاظ بالإصدارات السابقة من البرامج تحت إدارة التهيئة (Configuration Management) كإجراء احترازي.
- يجب الحفاظ على البرمجيات المزودة من الموردين والمستخدمة في بيئة الإنتاج، خاصة فيما يتعلق بتطبيق التصحيحات الأمنية.
- يجب تطوير خطة لإدارة الثغرات والتصحيحات الأمنية .(Vulnerability and Patch Management) ولا يجوز تطبيق التصحيحات على نظام الإنتاج إلا بعد اختبارها بنجاح في بيئة اختبار منفصلة.
- يُسمح بالوصول المباشر للقراءة فقط إلى برامج التطبيقات وملفات البيانات لأغراض إدارة الأنظمة الروتينية، مثل النسخ الاحتياطي، مراقبة الأداء والسعة، والمراقبة الأمنية. ولا يُسمح بأي وصول مباشر آخر إلا إذا تم التصريح به من خلال إجراءات التحكم في التغيير.

10.4 أمن الشيفرة المصدرية للبرامج

- يجب الاحتفاظ بالشيفرة المصدرية للبرامج والمعلومات المرتبطة بها (مثل التصاميم، المواصفات، قوائم البرامج، خطط الاختبار، والتقارير) بطريقة خاضعة للتحكم، كما يجب أن تتم الموافقة على التغييرات من قبل مالك الخدمة. يجب استخدام مكتبات منفصلة لبيئات التطوير والاختبار والإنتاج، وتكون تحت إدارة أشخاص مخوّلين.
- يجب اختبار الشيفرة البرمجية باستخدام أدوات تحليل الشيفرة والتحقق من اكتمالها. ولا يجوز إدراج الشيفرة في مكتبات الإنتاج إلا بعد إتمام اختبار القبول في بيئة الإنتاج.(Production Acceptance Testing)
- يجب تخزين الشيفرة في موقع مركزي ضمن مكتبات برمجية مؤمنة. كما يجب أن تكون تحديثات الشيفرة المخزنة في مكتبات الشيفرة المصدرية معتمدة من قبل مالك الخدمة. ويجب أن يتم إصدار أو ترجمة (Compile) الشيفرة من هذه المكتبات بواسطة أشخاص معينين، ويجب تسجيل هذه العمليات في سجلات رسمية.
- يجب أرشفة الإصدارات السابقة من البرامج المصدرية.
- يجب الاحتفاظ بالشيفرة المصدرية المملوكة لطرف ثالث في حساب ضمان (Escrow) إذا كانت التجارية تعتمد بشكل حرج على القدرة على صيانة/تحديث الشيفرة، وخاصة في حال وجود شكوك حول قدرة المورد أو استقراره.

10.5 حزم البرمجيات

- يجب أن يشترط عقد المورد الخارجي على البائع تأكيد إجراء اختبارات الأمان المناسبة، وأن تكون البرمجيات خالية من الثغرات الأمنية المعروفة.
- يجب استخدام حزم البرمجيات المقدمة من موردين خارجيين بدون تعديلات جوهرية متى ما كان ذلك ممكنًا.
- في حال اعتُبر من الضروري تعديل حزمة برمجيات مقدمة من طرف ثالث، يجب الالتزام بالقواعد التالية:
  - يجب الحصول على موافقة مسبقة من مالك الخدمة المعني والبائع.
  - يجب تقييم المخاطر المرتبطة والتأثيرات المحتملة، خاصةً إذا أصبحت التجارية مسؤولة عن صيانة البرمجيات في المستقبل نتيجة لهذا التغيير.
  - يجب اختبار التغييرات بالكامل والتحكم فيها.
  - يجب توثيق التغييرات بشكل كامل حتى يمكن إعادة تطبيقها إذا لزم الأمر بعد التحديثات المستقبلية التي يصدرها البائع.

10.6 أمن وثائق النظام

- يجب تصنيف الوثائق التي تصف تصميمات النظام والشبكة والتطبيقات، ومعايير الأمان، وعمليات التشغيل والإدارة، وهياكل البيانات، وإجراءات تفويض المستخدمين، وخطط الاختبار، ونتائج الاختبار، وفقًا لعملية تصنيف المعلومات المعتمدة لدى التجارية، وحمايتها بشكل كافٍ من الوصول غير المصرح به.
- يجب تطبيق إجراءات أمان مناسبة على وثائق النظام المخزنة على الإنترانت، والتي يمكن للموظفين الوصول إليها.

11. إدارة استمرارية الخدمة وتوفرها

تم تحديد السياسات في هذا القسم لوصف اعتبارات استمرارية الخدمات وتوفرها لدى التجارية. يجب إعداد خطط الطوارئ لعمليات الأعمال، بالإضافة إلى عمليات توفر واستعادة تكنولوجيا المعلومات، بهدف تعظيم القدرة على الحفاظ على مستوى عملي وفعّال من استمرارية الأعمال خلال الفترة الانتقالية بين انقطاع واستعادة خدمات تكنولوجيا المعلومات.

11.1 متطلبات استمرارية الخدمة وتوفرها

- يجب على التجارية تقييم وتوثيق المخاطر المتعلقة باستمرارية وتوفر خدمات تقنية المعلومات.
- يجب على التجارية التنسيق مع مختلف الأقسام لتحديد متطلبات استمرارية وتوفر خدمات تقنية المعلومات، مع مراعاة متطلبات الخدمة، اتفاقيات مستوى الخدمة (SLAs)، المخاطر، وخطط العمل.
- يجب أن تشمل متطلبات استمرارية وتوفر الخدمة ما يلي
  - أ- حقوق الوصول إلى الخدمات.
  - ب- أوقات الاستجابة للخدمة.
  - ت- توفر الخدمات من البداية للنهاية (End-to-end availability)

11.2 خطط استمرارية وتوفر الخدمة

يجب على التجارية توثيق وتنفيذ وصيانة الخطط والإجراءات الخاصة باستمرارية وتوفر الخدمة.

11.3 أمن المعلومات في إدارة استمرارية الأعمال

- يجب على التجارية إدارة استمرارية الأعمال بشكل مستمر عبر جميع أقسام الأعمال، مع التركيز على الاعتماد على العمليات التجارية الحيوية من خلال ضمان توفر نظم المعلومات الداعمة لها.
- يجب تحديد المكونات الحرجة لاستمرارية الخدمة، وتوفير الترتيبات اللازمة لتمكين استئناف الخدمات بسرعة في حال حدوث أي عطل.
- يجب تنفيذ الإجراءات التالية، حيثما أمكن، في مرافق معالجة المعلومات:
  - أ- توفير مصادر طاقة احتياطية.(Stand-by power supplies)
  - ب- توفير خوادم وأجهزة زائدة عن الحاجة.(Redundant servers and hardware)
  - ت- تكرار المعالجات والتخزين عبر الإنترنت.(Duplication of processors and on-line storage)
  - ث- إعادة توجيه الاتصالات تلقائيًا.(Automatic re-routing of communications)
  - ج- توفير القدرة على التحويل إلى خدمات إنترنت بديلة (Fall-back capability to alternative internet carrier services).
  - ح- الصيانة القائمة على العقود لضمان الإصلاح في الوقت المناسب (Contract-based maintenance to ensure timely repair).

12. التدريب والتوعية الأمنية

تهدف السياسات في هذا القسم إلى ضمان حصول موظفي التجارية على التدريب والتوعية المناسبة، وذلك لترسيخ التوقعات الأساسية لدى العاملين بشأن حماية أصول معلومات التجارية.

12.1 تعريف أمن المعلومات

- يجب وضع عملية تعريف شاملة لأمن المعلومات تقوم بتوضيح وتوصيل مسؤوليات وتوقعات أمن المعلومات للموظفين الذين يُفترض أن يكون لديهم وصول إلى أصول وأنظمة معلومات التجارية، وذلك بما يتناسب مع أدوارهم الوظيفية.
- يجب الاحتفاظ بسجلات توضح الأفراد الذين تلقوا تعريف أمن المعلومات. ويعد حضور جلسة تعريف الأمن شرطًا أساسيًا لمنح أي موظف جديد صلاحيات الوصول إلى أصول أو أنظمة المعلومات. ولا يُسمح بأي استثناءات.

12.2 الوعي العام بأمن المعلومات

- يجب أن يتم عقد جلسات توعية عامة بأمن المعلومات، التي تنطبق على موظفي شركة التجارية، مرة واحدة على الأقل سنويًا. يجب أن يتم التواصل حول أي تغييرات في عمليات تكنولوجيا المعلومات أو السياسات أو الهيكل التنظيمي مع المستخدمين خلال جلسات التوعية العامة، بالإضافة إلى وسائل الاتصال الأخرى المناسبة للأطراف المعنية في الوقت المناسب بعد التغيير.
- يجب أن يكون هناك تخطيط لعملية التواصل المتعلقة بأمن المعلومات، مع تحديد الجمهور المستهدف، وتواتر التواصل، ووسائل الاتصال المناسبة.
- يجب أن تشمل التوعية: أساليب التعاون الآمن والمشاركة الخارجية في Microsoft 365، وطرق التصدي للتصيد الاحتيالي والهندسة الاجتماعية، والتعامل الآمن مع تقنيات مواقع العمل، إضافة إلى متطلبات الاستخدام المقبول للذكاء الاصطناعي.

12.3 المنهج التعليمي والتدريبي لأمن المعلومات

- يجب تطوير منهج تدريبي لأمن المعلومات بالتنسيق مع إدارة الموارد البشرية، ويشمل الموظفين الذين يتعاملون مع أصول المعلومات وأنظمة شركة التجارية، مع تحديد الجلسات التدريبية اللازمة التي تتناسب مع الأدوار المرتبطة باستخدام أنظمة معلومات معينة.
- يجب تصميم المنهج التدريبي بناءً على نتائج التعلم والأهداف التي تتناسب مع الأدوار والفئات المختلفة من المعنيين. ويجب أن تقوم لجنة المخاطر والتدقيق بمراقبة تنفيذ المنهج التدريبي وفعالية التواصل المتعلق بأمن المعلومات، مثل حملات البريد الإلكتروني أو الإعلانات التوعوية، التي تذكر المستخدمين بالتزاماتهم المتعلقة بأمن المعلومات.
- يجب تطوير المنهج التدريبي لضمان عقد جلسات تدريبية سنوية لتعزيز وعي المستخدمين والأدوار الأخرى بمسؤولياتهم تجاه نظام إدارة أمن المعلومات.
- يجب على إدارة الموارد البشرية التنسيق بشكل وثيق مع قسم أمن المعلومات لضمان تحديث المنهج التدريبي ومواد التدريب لتعكس الاتجاهات الجديدة في أمن المعلومات، والتغيرات الكبيرة في بيئة شركة التجارية، والدروس المستفادة من الحوادث الأمنية السابقة، استنادًا إلى ملاحظات المشاركين.
- يجب تنظيم جلسات تدريبية متخصصة وفقًا للمنهج التدريبي.
- يجب أن تمكّن الجلسات التدريبية المتخصصة موظفي شركة التجارية والمستخدمين النهائيين من المساهمة بفعالية في تنفيذ وتحسين نظام إدارة أمن المعلومات، وفهم تبعات عدم الامتثال لمتطلبات سياسة أمن المعلومات.
- بالتنسيق مع إدارة الموارد البشرية، يجب إجراء تقييم بعد التدريب للتأكد من أن أهداف التدريب قد تم تحقيقها، وأن الحضور قد اكتسبوا المعرفة اللازمة لتطبيقها عمليًا.
- يجب على إدارة الموارد البشرية الاحتفاظ بسجلات الجلسات التدريبية المنفذة وحضور المشاركين. يجب أن يكون الحصول على التدريب المتخصص في حماية/إدارة نظام معلومات أو أصل معلومات معين شرطًا مسبقًا للحصول على الوصول إلى هذا النظام أو الأصل لأداء المهام المطلوبة.
- يجب توفير تدريب قائم على الأدوار لمالكي المعلومات ومديري المواقع/المشاريع، يشمل حوكمة المشاركة الخارجية في Microsoft 365، وإدارة وصول المقاولين من الباطن، والمسؤوليات المتعلقة بتصنيف المعلومات والاحتفاظ بها.