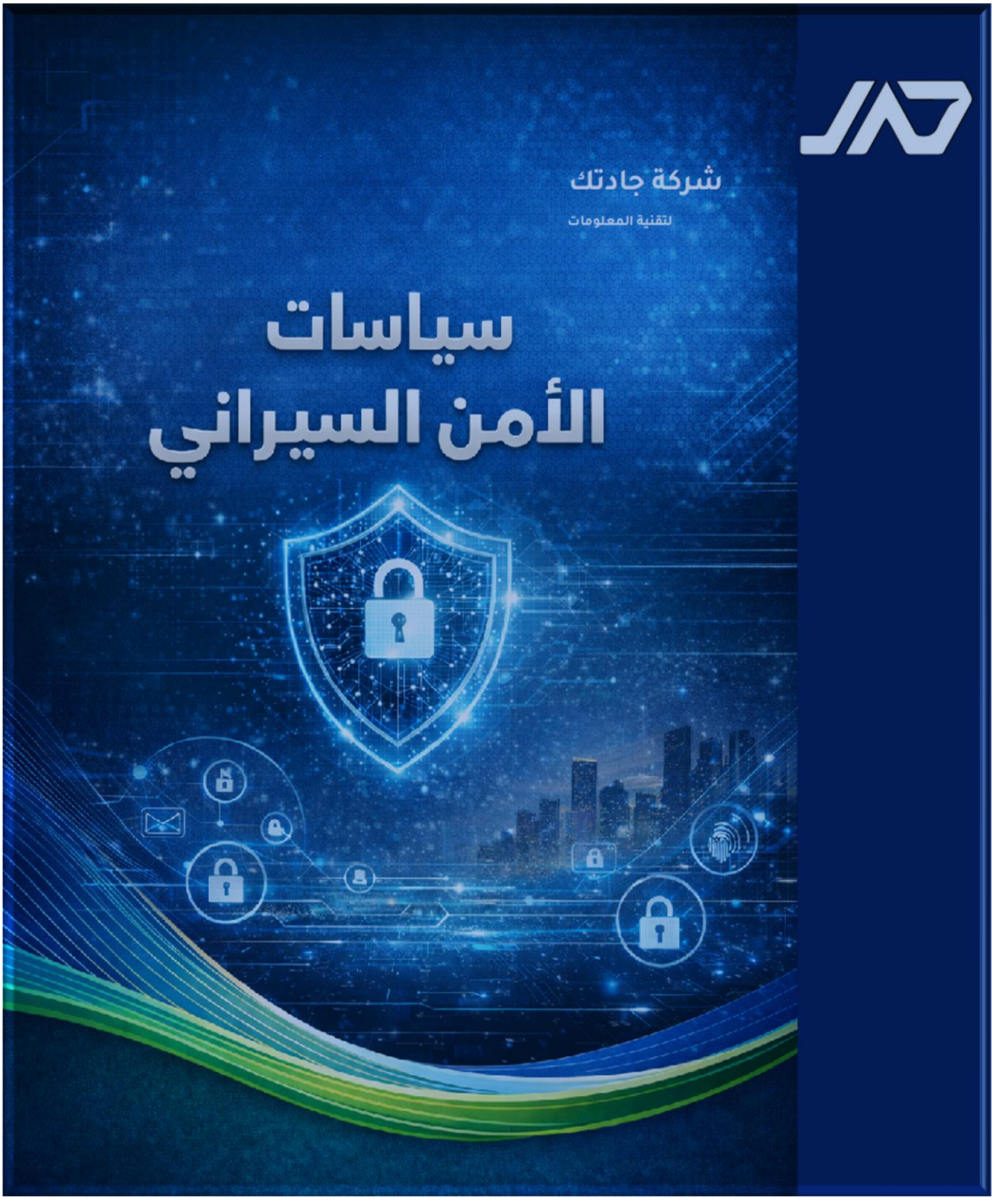
شركة جادتك

لتقنية المعلومات

سياسات الأمن السيراني



سياسات الامن السيبراني

المحتويات

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
المالك	المؤسس والمدير التنفيذي	حامد عاتق السهلي	2026/1/1	
المشرف	مدير التحول الرقمي	د. محمد عبد الرحيم يسن	2026/1/1	
المصرح	مدير الامن السيبراني	عبد الهادي القحطاني	2026/1/1	

نسخة الوثيقة

النسخة	التاريخ	عدل بواسطة	أسباب التعديل
1.0	2026/1/1	عبد الهادي القحطاني	النسخة الاولى
1.1	2026/4/5	عبد الهادي القحطاني	ملحق في النسخة الاولى

جدول المراجعة

معدل المراجعة	تاريخ آخر مراجعة	تاريخ المراجعة القادمة
مرة كل سنة	2026/1/1	2027/1/1

السياسات العامة للأمن السيبراني

الغرض

تهدف هذه السياسة إلى وضع المتطلبات العامة للأمن السيبراني داخل شركة جادتك، بما يضمن أن تكون السياسة الإطار الأساسي الذي تُبنى عليه جميع السياسات والمعايير والإجراءات الخاصة بالأمن السيبراني. كما تُعد هذه السياسة مرجعًا رئيسيًا يدعم عمليات الجهات الداخلية في الشركة، مثل إدارة الموارد البشرية، وإدارة الموردين، وإدارة المشاريع، وإدارة التغيير وتتماشى هذه السياسة مع الضوابط والمعايير الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تشمل هذه السياسة جميع الأصول المعلوماتية والتقنية التابعة لـ شركة جادتك، وتُطبّق على جميع العاملين في الشركة، سواء كانوا موظفين دائمين أو متعاقدين.

بنود السياسة

يتعيّن على الإدارة المختصة بالأمن السيبراني في شركة جادتك وضع وتطوير سياسات الأمن السيبراني، والمعايير التقنية، والأطر التنظيمية، إضافة إلى الإجراءات والضوابط اللازمة، اعتمادًا على مخرجات تقييم المخاطر. ويجب أن تسهم هذه السياسات في نشر متطلبات الأمن السيبراني والالتزام بتطبيقها، بما يتوافق مع احتياجات الأعمال والاشتراطات التنظيمية والتشريعية ذات الصلة. كما ينبغي اعتماد السياسات من قبل الرئيس التنفيذي في شركة جادتك أو من يمثله رسميًا، ثم تعميمها على الموظفين المعنيين والأطراف المرتبطة والمتعاقدين، لضمان فهمها وتطبيقها بالشكل المطلوب. والتي تتمثل فيما يلي:

سياسة إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Policy)

هي سياسة تهدف إلى وضع منهجية واضحة ومنظمة لتحديد مخاطر الأمن السيبراني التي قد تواجه شركة جادتك، وتحليلها وتقييم مستوى تأثيرها واحتمالية حدوثها، ثم معالجتها وفق إطار معتمد يقلل من تأثير التهديدات السيبرانية على أصول الشركة وعملياتها. وتهدف هذه السياسة إلى تعزيز القدرة على التنبؤ بالمخاطر، واتخاذ قرارات مبنية على معلومات دقيقة، وضمان استمرارية الأعمال ورفع مستوى الحماية السيبرانية في الشركة.

سياسة دورة حياة تطوير البرمجيات الآمنة (Secure Software Development Lifecycle Policy)

هي سياسة تهدف إلى تطبيق منهجية واضحة ومنظمة لضمان اتباع ممارسات تطوير آمنة في جميع مراحل دورة حياة البرمجيات داخل شركة جادتك، بدءًا من تحليل المتطلبات والتصميم، مرورًا بالتطوير والاختبار، وانتهاءً بمرحلة النشر والصيانة، بما يسهم في تقليل

الثغرات الأمنية ورفع جودة الأنظمة والتطبيقات، وضمان توافقها مع المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة الإعدادات والتحصين (Configuration and Hardening Policy)

هي سياسة تهدف إلى وضع منهجية واضحة ومنظمة لضمان تطبيق إعدادات آمنة وتحسين مستوى التحصين على الأنظمة والأجهزة والخوادم والتطبيقات داخل شركة جادتك، وذلك من خلال تقييد الإعدادات الافتراضية، وتقليل نقاط الضعف، وتعزيز مستوى الحماية الفنية في بيئة الشركة. وتهدف هذه السياسة إلى رفع جاهزية البنية التحتية، وتقليل مخاطر الاستغلال السيبراني، وضمان التوافق مع أفضل الممارسات والمعايير الأمنية المعتمدة.

سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني (Cybersecurity Laws and Regulations Compliance Policy)

هي سياسة تهدف إلى ضمان التزام **شركة جادتك** بجميع التشريعات والأنظمة والمتطلبات التنظيمية المرتبطة بالأمن السيبراني والصادرة من الجهات المختصة، من خلال تطبيق الضوابط والإجراءات التي تضمن الامتثال الكامل وتحديثه بشكل مستمر. وتهدف هذه السياسة إلى حماية الشركة من المخاطر النظامية، وتعزيز الموثوقية، وضمان توافق عملياتها مع الإطار التشريعي والتنظيمي المعتمد.

سياسة مراجعة وتدقيق الأمن السيبراني (Cybersecurity Review and Audit Policy)

هي سياسة تهدف إلى وضع آلية واضحة ومستمرة لمراجعة وتقييم فعالية ضوابط الأمن السيبراني داخل شركة جادتك، وذلك من خلال إجراء تدقيقات دورية داخلية وخارجية للتأكد من التزام الأنظمة والبنية التحتية والسياسات بالمعايير والممارسات الأمنية المعتمدة. وتهدف هذه السياسة إلى كشف الثغرات وتحسين القدرات الأمنية ورفع مستوى النضج السيبراني في الشركة من خلال التوصيات والإجراءات التصحيحية المستمرة.

سياسة الأمن السيبراني للموارد البشرية (Human Resources Cybersecurity Policy)

هي سياسة تهدف إلى تنظيم وإدارة متطلبات الأمن السيبراني المتعلقة بدورة حياة الموظفين في شركة جادتك، وذلك من خلال تطبيق ضوابط واضحة تشمل مراحل ما قبل التوظيف، وأثناء الخدمة، وما بعد انتهاء العلاقة الوظيفية، بما يضمن حماية أصول الشركة ومعلوماتها وتقليل المخاطر المرتبطة بالأفراد. وتهدف هذه السياسة إلى تعزيز الوعي الأمني، وضمان الالتزام بالسلوكيات الآمنة، ودعم بيئة عمل آمنة تتوافق مع المعايير والسياسات السيبرانية المعتمدة في الشركة.

سياسة الاستخدام المقبول للأصول (Acceptable Use of Assets Policy)

هي سياسة تهدف إلى تحديد القواعد والضوابط التي تحكم كيفية استخدام الأصول التقنية والمعلوماتية التابعة لـ شركة جادتك، بما في ذلك الأجهزة، الشبكات، الأنظمة، التطبيقات، والبيانات. وتوضح هذه السياسة السلوكيات المقبولة والممنوعة عند استخدام الأصول لضمان الحفاظ على أمن المعلومات، وتقليل المخاطر التشغيلية، وتعزيز الاستخدام المسؤول لهذه الموارد، بما يتوافق مع المعايير والسياسات الأمنية المعتمدة في الشركة.

سياسة إدارة هويات الدخول والصلاحيات (Identity and Access Management Policy)

هي سياسة تهدف إلى تنظيم وضبط آليات إدارة هويات المستخدمين وتحديد مستويات الصلاحيات داخل شركة جادتك، وذلك من خلال وضع ضوابط واضحة لعمليات إنشاء الحسابات، وتعديلها، ومراجعتها، وتعطيلها، بالإضافة إلى تحديد آليات التحكم في الوصول إلى الأنظمة والأصول المعلوماتية. وتهدف هذه السياسة إلى ضمان منح الصلاحيات وفق مبدأ الحاجة إلى المعرفة، وتقليل مخاطر الوصول غير المصرح به، وتعزيز حماية البيانات والأنظمة وفق أفضل الممارسات الأمنية المعتمدة في الشركة.

سياسة أمن قواعد البيانات (Database Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لضمان حماية قواعد البيانات في شركة جادتك، وذلك من خلال تنظيم آليات الوصول، وتطبيق معايير التشفير، وتعزيز المراقبة، وحماية سلامة البيانات وتوافرها وسريتها. وتهدف هذه السياسة إلى تقليل مخاطر الاختراق أو التلاعب بالبيانات، وضمان تشغيل قواعد البيانات ضمن بيئة آمنة ومتوافقة مع أفضل الممارسات والمعايير الأمنية المعتمدة في الشركة.

سياسة أمن الخوادم (Server Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية الخوادم في شركة جادتك، وذلك من خلال تطبيق ممارسات التحصين، وإعداد الإعدادات الآمنة، وتنظيم آليات الوصول، ومراقبة الأنشطة، وضمان تحديث الخوادم بشكل مستمر. وتهدف هذه السياسة إلى حماية البنية التحتية للخوادم من التهديدات السيبرانية، وتقليل مخاطر الاستغلال، وضمان استمرارية عمل الأنظمة والخدمات ضمن بيئة آمنة تتوافق مع أفضل المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة الحماية من البرمجيات الضارة (Malware Protection Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات فعّالة لحماية أنظمة وأصول شركة جادتك من البرمجيات الضارة بجميع أنواعها، وذلك من خلال اعتماد حلول كشف ومنع التهديدات،

وتطبيق آليات الفحص المستمر، وتعزيز مراقبة الأنشطة المشبوهة، وتحديث أدوات الحماية بشكل دوري. وتهدف هذه السياسة إلى تقليل مخاطر الإصابة بالبرامج الخبيثة، وضمان سلامة الأنظمة والبيانات، ورفع مستوى الاستجابة والجاهزية ضد أي تهديدات سيبرانية محتملة.

سياسة حزم التحديثات والإصلاحات (Patch Management Policy)

هي سياسة تهدف إلى وضع آلية واضحة ومنظمة لإدارة وتطبيق التحديثات والإصلاحات الأمنية على الأنظمة والأجهزة والتطبيقات داخل شركة جادتك، وذلك لضمان معالجة الثغرات وتحسين الأداء وتقليل المخاطر السيبرانية الناتجة عن الإصدارات غير المحدثة. وتهدف هذه السياسة إلى ضمان استمرارية عمل الأنظمة بكفاءة، وتعزيز مستوى الحماية، والالتزام بأفضل الممارسات في إدارة التحديثات والإصلاحات ضمن بيئة الشركة.

سياسة أمن وسائط التخزين(Storage Media Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية وسائط التخزين المستخدمة داخل شركة جادتك، سواء كانت وسائط داخلية أو خارجية، وذلك من خلال تنظيم أساليب استخدامها، وتطبيق معايير التشفير، والتحكم في الوصول، وضمان التخلص الآمن منها. وتهدف هذه السياسة إلى حماية المعلومات من الفقدان أو التسريب أو الوصول غير المصرح به، وتعزيز أمن البيانات المخزنة وفق أفضل الممارسات والمعايير الأمنية المعتمدة في الشركة.

سياسة أمن البريد الإلكتروني(Email Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لضمان الاستخدام الآمن للبريد الإلكتروني داخل شركة جادتك، وذلك من خلال تنظيم آليات الإرسال والاستقبال، وحماية حسابات البريد من محاولات التصيدphishing ، وتطبيق معايير التحقق، ومراقبة الرسائل والروابط والملفات المشبوهة. وتهدف هذه السياسة إلى حماية الأنظمة والمستخدمين من التهديدات المرتبطة بالبريد الإلكتروني، وتقليل مخاطر الاختراق أو تسريب المعلومات، وضمان التوافق مع أفضل الممارسات الأمنية المعتمدة في الشركة.

سياسة أمن الشبكات(Network Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية شبكات شركة جادتك من التهديدات السيبرانية، وذلك من خلال تنظيم آليات الوصول، وتطبيق أنظمة الحماية والمراقبة، وتعزيز مستوى التحصين، وضمان سلامة حركة البيانات داخل الشبكة. وتهدف هذه السياسة إلى تقليل مخاطر الاختراق أو التلاعب بالاتصالات، وضمان استمرارية الخدمات،

وحماية البنية التحتية للشبكة بما يتوافق مع أفضل المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والشخصية (Endpoint and Mobile Devices Security Policy)

وهي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية أجهزة المستخدمين في شركة جادتك، بما في ذلك الأجهزة المكتبية والمحمولة والأجهزة الشخصية المصرّح باستخدامها، وذلك من خلال تطبيق آليات التحصين، والتحكم في الوصول، وتحديث الأنظمة، وتفعيل أدوات الحماية والمراقبة. وتهدف هذه السياسة إلى تقليل مخاطر الاختراق أو فقدان البيانات، وضمان استخدام آمن للأجهزة التي تصل إلى شبكات وأنظمة الشركة، بما يتوافق مع أفضل الممارسات والمعايير الأمنية المعتمدة.

سياسة الأمن السيبراني للبيانات(Data Cybersecurity Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية البيانات داخل شركة جادتك طوال دورة حياتها، وذلك من خلال تنظيم أساليب تصنيف البيانات، وتخزينها، ونقلها، والوصول إليها، والاحتفاظ بها، والتخلص منها بشكل آمن. وتهدف هذه السياسة إلى ضمان سرية البيانات وسلامتها وتوافرها، وتقليل مخاطر التسريب أو التلاعب، وتعزيز مستوى الحماية بما يتوافق مع أفضل المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة التشفير (Encryption Policy)

هي سياسة تهدف إلى وضع ضوابط وآليات واضحة لتطبيق التشفير على البيانات والأصول المعلوماتية داخل شركة جادتك، سواء أثناء التخزين أو أثناء النقل، وذلك لضمان حماية البيانات من الوصول غير المصرح به أو من أي عمليات اعتراض أو اختراق محتملة. وتهدف هذه السياسة إلى تعزيز سرية المعلومات وسلامتها، وضمان استخدام تقنيات التشفير المعتمدة بما يتوافق مع أفضل الممارسات والمعايير الأمنية المطبقة في الشركة.

سياسة النسخ الاحتياطي(Backup Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لإجراء النسخ الاحتياطي للبيانات والأنظمة في شركة جادتك، وذلك لضمان حفظ نسخ آمنة من المعلومات الهامة واستعادتها عند الحاجة، سواء في حالات الطوارئ أو الأعطال أو فقدان البيانات. وتهدف هذه السياسة إلى تعزيز استمرارية الأعمال، وتقليل مخاطر فقدان المعلومات، وضمان تنفيذ عمليات النسخ الاحتياطي والاستعادة وفق معايير وممارسات أمنية معتمدة في الشركة.

سياسة إدارة الثغرات(Vulnerability Management Policy)

هي سياسة تهدف إلى وضع آلية واضحة ومنهجية لاكتشاف الثغرات الأمنية في أنظمة وشبكات وتطبيقات شركة جادتك، وتقييم مستوى خطورتها، ومعالجتها ضمن إطار زمني معتمد يقلل من احتمالية الاستغلال السيبراني. وتهدف هذه السياسة إلى تعزيز حماية البنية التحتية التقنية، وتقليل المخاطر الناتجة عن الثغرات، وضمان الالتزام بأفضل الممارسات والمعايير الأمنية في إدارة الثغرات داخل الشركة.

سياسة اختبار الاختراق(Penetration Testing Policy)

هي سياسة تهدف إلى وضع منهجية واضحة لتنفيذ اختبارات الاختراق على أنظمة وشبكات وتطبيقات شركة جادتك، وذلك بهدف اكتشاف الثغرات الأمنية المحتملة وتقييم مستوى مقاومتها للهجمات السيبرانية. وتشمل السياسة تحديد نطاق الاختبار، والجهات المخوّلة بالتنفيذ، وآليات المعالجة والمتابعة. وتهدف هذه السياسة إلى تعزيز جاهزية الأنظمة، وتقليل مخاطر الاستغلال، وضمان توافق عمليات الاختبار مع أفضل الممارسات والمعايير الأمنية المعتمدة في الشركة.

سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Security Logging and Monitoring Policy)

هي سياسة تهدف إلى وضع ضوابط وآليات واضحة لجمع سجلات الأحداث وتحليلها ومراقبة الأنشطة داخل أنظمة وشبكات شركة جادتك، وذلك للكشف المبكر عن التهديدات والهجمات السيبرانية والاستجابة لها بشكل فعّال. وتشمل هذه السياسة تحديد أنواع السجلات المطلوبة، وآليات الاحتفاظ بها، والمسؤوليات المتعلقة بمراجعتها وتحليلها. وتهدف إلى تعزيز قدرة الشركة على اكتشاف الحوادث، وتحسين الاستجابة، ورفع مستوى الحماية وفق أفضل الممارسات والمعايير الأمنية المعتمدة.

سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management Policy)

هي سياسة تهدف إلى وضع إطار واضح ومنظم لرصد وتحديد ومعالجة حوادث وتهديدات الأمن السيبراني التي قد تستهدف أنظمة وشبكات وتطبيقات شركة جادتك، وذلك من خلال وضع آليات اكتشاف مبكر، وخطط استجابة، وإجراءات احتواء، ومعالجة، واستعادة، إضافة إلى توثيق الحوادث وتحليل أسبابها لمنع تكرارها. وتهدف هذه السياسة إلى رفع جاهزية الشركة للاستجابة الفعّالة للـ incident، وتقليل الأثر المحتمل، وتحسين القدرة الدفاعية وفق أفضل المعايير والممارسات الأمنية المعتمدة.

سياسة الأمن السيبراني المتعلقة بالأمن المادي(Physical Security Cyber Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لحماية الأصول والمرافق المادية في شركة جادتك من الوصول غير المصرح به أو العبث أو التهديدات البيئية، وذلك من خلال تنظيم آليات التحكم في الدخول، وأنظمة المراقبة، والتدابير الوقائية داخل المواقع الحساسة مثل غرف الخوادم ومراكز البيانات. وتهدف هذه السياسة إلى تعزيز الترابط بين الأمن المادي والأمن السيبراني لضمان حماية شاملة للأصول وتقليل المخاطر وضمان استمرارية الأعمال وفق أفضل المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة حماية تطبيقات الويب(Web Application Security Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لتعزيز أمن تطبيقات الويب التابعة لـ **شركة جادتك**، وذلك من خلال تطبيق ممارسات تطوير آمن، وتنفيذ اختبارات أمنية دورية، ومعالجة الثغرات، وضمان حماية الطبقات المختلفة للتطبيق من الهجمات الشائعة مثل حقن الأكواد وهجمات التصيد والإستغلالات المباشرة. وتهدف هذه السياسة إلى رفع مستوى أمان تطبيقات الويب، وتقليل مخاطر الاختراق أو التلاعب بالبيانات، وضمان توافق عمليات تطوير وتشغيل التطبيقات مع أفضل المعايير والممارسات الأمنية المعتمدة في الشركة.

سياسة الأمن السيبراني ضمن استمرارية الأعمال(Cybersecurity Business Continuity Policy)

هي سياسة تهدف إلى ضمان دمج متطلبات الأمن السيبراني داخل خطط استمرارية الأعمال في شركة جادتك، وذلك من خلال تحديد الضوابط والإجراءات اللازمة لحماية الأنظمة والبيانات أثناء الأزمات والطوارئ، وضمان استعادة الخدمات الحيوية ضمن إطار زمني معتمد. وتهدف هذه السياسة إلى تقليل تأثير الحوادث السيبرانية على العمليات التشغيلية، وتعزيز جاهزية الشركة للاستجابة والتعافي، وضمان استمرارية الأعمال وفق أفضل الممارسات والمعايير الأمنية المعتمدة.

سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party Cybersecurity Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لتنظيم وإدارة متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية التي تتعامل مع شركة جادتك أو تحصل على وصول إلى أنظمتها أو بياناتها، وذلك من خلال تقييم مخاطر الموردين، وتحديد الالتزامات الأمنية، ومراقبة الامتثال، وضمان حماية المعلومات أثناء تعاملات وخدمات الأطراف الخارجية. وتهدف هذه

السياسة إلى تقليل المخاطر الناتجة عن مقدمي الخدمات والشركاء، وضمان التزامهم بأفضل الممارسات والمعايير الأمنية المعتمدة في الشركة.

سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity Policy)

هي سياسة تهدف إلى وضع ضوابط وإجراءات واضحة لتنظيم استخدام وخدمات الحوسبة السحابية وخدمات الاستضافة في شركة جادتك، وذلك من خلال تحديد معايير الأمان المطلوبة، وضوابط حماية البيانات، وإدارة الوصول، وآليات مراقبة مقدمي الخدمات السحابية، وضمان الامتثال للمتطلبات التنظيمية. وتهدف هذه السياسة إلى حماية الأصول والبيانات المخزّنة أو المعالجة عبر البيئات السحابية، وتقليل المخاطر المرتبطة بالخدمات المستضافة، وضمان توافقها مع أفضل الممارسات والمعايير الأمنية المعتمدة في الشركة.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها.
مسؤول الأمن السيبراني	تنفيذ السياسة، مراقبة الأنظمة، التحقيق في الحوادث، ورفع التقارير.
الموظفون والمستخدمون	الالتزام بالسياسة، الحفاظ على المعلومات، الإبلاغ عن أي سلوك غير اعتيادي.
قسم تقنية المعلومات	تطبيق الضوابط التقنية، إدارة الصلاحيات، ضبط النسخ الاحتياطي وتحديث الأنظمة.

الالتزام بالسياسة

- يعد الالتزام بهذه السياسة إلزامياً على جميع موظفي شركة جادتك والمتعاملين معها.
- قد يؤدي عدم الالتزام إلى اتخاذ إجراءات إدارية أو قانونية بحسب خطورة المخالفة.
- تتم مراجعة هذه السياسة سنوياً أو عند الحاجة لضمان ملاءمتها للتغيرات التقنية والتنظيمية.

1- سياسة إدارة مخاطر الأمن السيبراني

الغرض

تهدف هذه السياسة إلى وضع إطار واضح لتحديد وتقييم ومعالجة ومراقبة مخاطر الأمن السيبراني في شركة جادتك، لضمان حماية أصول المعلومات وتقليل التأثير المحتمل للحوادث الأمنية على استمرارية الأعمال وسمعة شركة جادتك.

المرجع: الضابط الأمني رقم 1-5 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع الأقسام والموظفين والمتعاقدين.
- جميع أصول الشركة المعلوماتية (بيانات، أنظمة، شبكات، تطبيقات، أجهزة).
- العمليات والخدمات الرقمية التي تعتمد عليها شركة جادتك.
- الأطراف الثالثة المزودة للخدمات التقنية أو الشريكة في تبادل البيانات.

بنود السياسة

1-1تحديد المخاطر

1-1-1 يجب تحديد الأصول المعلوماتية الحيوية وتقييم مستوى حساسيتها.

2-1-1 تحليل التهديدات المحتملة ونقاط الضعف المرتبطة بها.

2-1 تقييم المخاطر

1-2-1 يتم تقييم المخاطر بناءً على احتمالية حدوثها وتأثيرها.

2-2-1 تصنيف المخاطر إلى مستويات (منخفض - متوسط - عالي - حرج).

3-1 معالجة المخاطر

1-3-1 اختيار طريقة التعامل مع كل خطر (تجنب - تقليل - نقل - قبول).

2-3-1 تطبيق ضوابط أمنية مناسبة للحد من المخاطر العالية والحرجة.

4-1 مراقبة المخاطر ومراجعتها

1-4-1 مراجعة المخاطر بشكل دوري أو عند حدوث تغييرات في الأنظمة أو العمليات.

2-4-1 تحديث تقارير المخاطر بشكل مستمر ورفعها للإدارة.

5-1 توثيق الإجراءات

1-5-1 الاحتفاظ بسجلات المخاطر وخطط المعالجة والنتائج في نظام موحد.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد سياسة إدارة المخاطر وتوفير الموارد اللازمة.
مسؤول الأمن السيبراني	قيادة عملية تقييم المخاطر، تحديث سجلاتها، ومتابعة تنفيذ خطط المعالجة.
قسم تقنية المعلومات	تطبيق الحلول الأمنية وتحديث الأنظمة وتقديم تقارير فنية دورية.
جميع الموظفين	الالتزام بإجراءات الأمان، والإبلاغ عن أي مخاطر أو سلوكيات تهدد أمن المعلومات.
الأطراف الخارجية (إن وجدت)	الامتثال لمتطلبات أمان شركة جادتك وبنود العقود المتعلقة بحماية البيانات.

الالتزام بالسياسة

- يعتبر الالتزام بهذه السياسة إلزامياً لجميع العاملين والمتعاملين مع شركة جادتك.
- أي انتهاك قد يؤدي إلى إجراءات إدارية أو قانونية بحسب نوع المخالفة.
- تتم مراجعة السياسة سنوياً أو عند تغيير طبيعة الأعمال أو المخاطر.

2- سياسة دورة حياة تطوير البرمجيات الآمنة

الغرض

تهدف هذه السياسة إلى ضمان تطوير البرمجيات بطريقة آمنة من مرحلة التصميم وحتى النشر والصيانة، بهدف حماية البيانات والأنظمة من الثغرات والهجمات السيبرانية، وتقليل المخاطر المرتبطة بالبرمجيات المستخدمة داخل شركة جادتك أو البرمجيات المقدمة للعملاء.

المرجع: الضابط الأمني رقم 1-6 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع فرق تطوير البرمجيات (داخليًا وخارجيًا).
- جميع المشاريع البرمجية والتطبيقات والمواقع والخدمات الرقمية التي تطورها شركة جادتك.
- جميع مراحل دورة حياة تطوير البرمجيات: التخطيط، التصميم، البرمجة، الاختبار، النشر، الصيانة.

بنود السياسة

1-2 التخطيط والتصميم الأمني

2-1-1 يجب تحليل المخاطر الأمنية وتحديد المتطلبات الأمنية قبل البدء بالتصميم.

2-1-2 اعتماد المعايير الأمنية مثل OWASP و ISO/IEC 27001عند تصميم الأنظمة.

2-2 البرمجة الآمنة

2-2-1 كتابة التعليمات (الاكواد) البرمجية وفق أفضل الممارسات الأمنية.

2-2-2 تجنب الثغرات المعروفة مثلSQL Injection ، XSS، CSRF.

2-2-3 استخدام أدوات فحص الأمان الآلي.(Static & Dynamic Analysis Tools)

3-2 اختبار الأمان

2-3-1 إجراء اختبارات أمان شاملة قبل نشر أي إصدار، تشمل اختبارات الاختراق والفحص الأمني.

2-3-2 توثيق نتائج الاختبارات ومعالجة الثغرات المكتشفة قبل الإطلاق.

2-4 النشر والإصدار

2-4-1 التأكد من تكوين الأنظمة والتطبيقات بشكل آمن قبل نشرها.

2-4-2 الاحتفاظ بنسخ احتياطية من الإصدارات المهمة.

2-4-3 مراقبة الأنظمة بعد النشر للكشف عن أي نشاط غير طبيعي.

2-5 الصيانة والدعم

2-5-1 تحديث البرمجيات بشكل دوري لإصلاح الثغرات المكتشفة.

2-5-2 مراجعة الأكواد والإعدادات الأمنية بشكل دوري لضمان الاستمرار بالأمان.

2-5-3 إبلاغ الفرق المعنية عند اكتشاف أي ضعف أمني أو هجوم محتمل.

2-6 التوثيق والمراجعة

2-6-1 توثيق جميع مراحل تطوير البرمجيات الأمنية.

2-6-2 إجراء مراجعات دورية لسياسة التطوير الأمني لضمان التوافق مع المعايير الحديثة.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة للتطوير الآمن.
مدير المشاريع / فريق التطوير	ضمان تطبيق أفضل الممارسات الأمنية في جميع مراحل SDLC.
مسؤول الأمن السيبراني	تقييم المخاطر، إجراء اختبارات الأمان، تقديم التوجيه الفني للفريق.
قسم تقنية المعلومات	دعم البيئة التقنية، توفير الأدوات اللازمة للفحص الأمني، متابعة التحديثات.
الموظفون والمطورون	الالتزام بالسياسات والإرشادات الأمنية أثناء تطوير البرمجيات.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع فرق التطوير والمطورين والمتعاقدين.
- أي مخالفة أو تجاهل لإجراءات الأمان قد يؤدي إلى اتخاذ إجراءات إدارية أو قانونية.
- مراجعة السياسة بشكل دوري أو عند إدخال تقنيات جديدة لضمان ملاءمتها وحماية الأنظمة من التهديدات الحديثة.

3- سياسة الاعدادات والتحصين

الغرض

تهدف هذه السياسة إلى ضمان إعداد وتكوين الأنظمة والأجهزة والتطبيقات بطريقة آمنة تقلل من الثغرات والتهديدات السيبرانية، من خلال تطبيق أفضل ممارسات التحصين وتعزيز حماية البنية التحتية التقنية لشركة جادتك.

المرجع: الضابط الأمني رقم 1-6 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع الخوادم، وأجهزة المستخدمين، والشبكات، والتطبيقات، وقواعد البيانات.
- جميع الأنظمة الجديدة قبل تشغيلها أو تحديثها.
- كافة موظفي قسم تقنية المعلومات ومسؤولي الأنظمة والصيانة والدعم.

بنود السياسة

1-3 تحصين الأنظمة قبل الاستخدام

1-1-3 يجب إزالة أو تعطيل الخدمات والتطبيقات غير الضرورية قبل تشغيل أي نظام.

2-1-3 تفعيل إعدادات الأمان الافتراضية المقترحة من الشركات المصنعة.

2-3 تحديث الأنظمة

1-2-3 تثبيت التحديثات الأمنية بشكل دوري أو فور توفرها للأنظمة والبرامج.

2-2-3 التأكد من تطبيق التصحيحات المتعلقة بالثغرات الحرجة فوراً.

3-3 التحكم في المنافذ والخدمات

1-3-3 مسح المنافذ المفتوحة وتقليلها إلى أدنى حد.

2-3-3 السماح فقط بالخدمات الضرورية للعمل، ومنع أو إغلاق أي خدمات غير مستخدمة.

4-3 إعداد جدران الحماية ومكافحة البرمجيات الضارة

1-4-3 تفعيل جدار حماية داخلي وخارجي ومراقبة إعداداته بشكل مستمر.

3-4-2 تثبيت نظام حماية من الفيروسات والبرمجيات الضارة مع تحديثه تلقائياً.

3-5 تطبيق سياسات كلمات المرور والمصادقة

3-5-1 استخدام كلمات مرور موثوقة وتفعيل المصادقة متعددة العوامل (MFA) حيثما أمكن.

3-5-2 تعطيل أو حذف الحسابات غير النشطة أو غير المستخدمة.

3-6 مراقبة وتدقيق الإعدادات

3-6-1 إجراء مراجعات وتدقيقات دورية لضبط الإعدادات والتحصين.

3-6-2 الاحتفاظ بسجلات الأحداث (Logs) ومراقبتها للكشف المبكر عن أي نشاط غير طبيعي.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
قسم تقنية المعلومات	تنفيذ عمليات التحصين، متابعة التحديثات الأمنية، مراجعة الإعدادات بشكل دوري.
مسؤول الأمن السيبراني	تقييم جاهزية الأنظمة، إجراء تدقيقات أمنية، تقديم التوصيات ومراقبة الالتزام.
الموظفون	استخدام الأنظمة وفق الإعدادات المعتمدة وعدم تغييرها دون إذن.

الالتزام بالسياسة

- يعد تطبيق هذه السياسة إلزامياً على جميع الموظفين والجهات الفنية.
- أي تعديل على إعدادات الأنظمة دون إذن رسمي يعد مخالفة أمنية تستوجب اتخاذ الإجراءات الإدارية او القانونية.
- تتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع التغيرات التقنية والتهديدات الحديثة.

4- سياسة الالتزام بتشريعات وتنظيمات الامن السيبراني

الغرض

تهدف هذه السياسة إلى ضمان التزام شركة جادتك بجميع الأنظمة والقوانين والتشريعات والضوابط الخاصة بالأمن السيبراني الصادرة عن الجهات الوطنية والدولية ذات العلاقة، وذلك لضمان حماية أصول المعلومات وتقليل المخاطر والامتثال لمتطلبات الحوكمة والرقابة.

المرجع: الضابط الأمني رقم 1-7 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع موظفي شركة جادتك والمتعاقدين والزوار الذين لهم حق الوصول إلى الأنظمة أو البيانات.
- جميع الأنظمة والتطبيقات والبنية التحتية التقنية التابعة لشركة جادتك.
- جميع العمليات والإجراءات المتعلقة بمعالجة أو نقل أو تخزين المعلومات.

بنود السياسة

1-4 الالتزام بالأنظمة المحلية

1-1-4 الالتزام بجميع التشريعات الوطنية مثل سياسات الأمن السيبراني الصادرة عن الجهات الحكومية والهيئات التنظيمية.

2-1-4 تطبيق ضوابط "الهيئة الوطنية للأمن السيبراني (NCA) "ومتطلباتها الفنية والتنظيمية عند توفرها.

2-4 تطبيق أفضل المعايير الدولية

1-2-4 اعتماد أفضل ممارسات الأمن السيبراني مثل ISO/IEC 27001 و NIST عند تصميم وتطوير نظم الأمن الداخلي.

5-4 تقييم الالتزام بشكل دوري

1-5-4 إجراء مراجعات وتقييمات دورية للتأكد من توافق الأنظمة والإجراءات مع التشريعات الحالية.

2-5-4 معالجة أي حالات عدم امتثال في الفترة الزمنية المحددة.

4-4 التواصل والمتابعة

4-4-1 متابعة أي تحديث أو إصدار تشريعي جديد في مجال الأمن السيبراني.

4-4-2 إبلاغ الإدارات المعنية وتحديث الإجراءات والسياسات وفق ذلك.

5-4 التدريب والتوعية

4-5-1 توفير برامج تدريب وتوعية للموظفين حول المتطلبات القانونية ذات الصلة بالأمن السيبراني.

4-5-1 التأكد من فهم الموظفين لواجباتهم المتعلقة بالامتثال.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة، الإشراف على الالتزام، وتوفير الموارد اللازمة.
مسؤول الأمن السيبراني	متابعة وتفسير التشريعات، تحديث السياسات، تنفيذ الرقابة، وإجراء التقييمات الدورية.
الإدارات التقنية والتشغيلية	تطبيق الإجراءات اللازمة لضمان الالتزام بالتشريعات ضمن أعمالها.
الموظفون	فهم واتباع هذه السياسة والامتناع عن أي ممارسة تخالف التشريعات المعتمدة.

الالتزام بالسياسة

- يعتبر الالتزام بهذه السياسة إلزاميًا لجميع جهات وموظفي شركة جادتك.
- أي مخالفة قد يعرض شركة جادتك لعقوبات قانونية أو مخاطر تشغيلية.
- سيتم اتخاذ الإجراءات المناسبة بحق أي موظف أو جهة داخلية لا تلتزم بتنفيذ هذه السياسة.
- يتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع التغييرات التشريعية والتقنية.

5- سياسة مراجعة وتدقيق الأمن السيبراني

الغرض

تهدف هذه السياسة إلى وضع إطار واضح ومنظم لعمليات مراجعة وتدقيق الأمن السيبراني داخل شركة جادتك، وذلك بهدف تقييم كفاءة الضوابط الأمنية، واكتشاف الثغرات والمخاطر، وتحسين مستوى حماية الأنظمة والمعلومات، والالتزام بأفضل المعايير والممارسات المتبعة.

المرجع: الضابط الأمني رقم 1-8 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع أنظمة وتقنيات المعلومات، والتطبيقات، والشبكات، وقواعد البيانات.
- جميع الإدارات والأقسام المعنية بتشغيل أو إدارة أو استخدام الأنظمة التقنية.
- مقدمي الخدمات والمتعاقدين الخارجيين إذا كان لهم وصول إلى أصول معلومات شركة جادتك.

بنود السياسة

5-1مراجعات دورية

5-1-1 يجب إجراء مراجعات وتدقيقات أمنية على الأنظمة والبنية التحتية بشكل دوري وفق خطة معتمدة مسبقاً.

5-1-2 يتم تحديد تكرار المراجعات والتدقيقات الامنية بناء على مستوى المخاطر، بحد أدنى مرة واحدة سنوياً.

5-2 تقييم المخاطر

5-2-1 إجراء تقييم مخاطر شامل قبل وبعد أي تغيير رئيسي في الأنظمة أو المشاريع.

5-2-2 استخدام نتائج التقييم لتطوير إجراءات وقائية وتحسين الضوابط الأمنية.

5-3 اختبارات الاختراق

5-3-1 تنفيذ اختبارات اختراق داخلية وخارجية دورية لتحديد نقاط الضعف ومعالجتها.

5-3-2 يتم تنفيذ هذه الاختبارات بواسطة جهات مختصة معتمدة.

4-5 توثيق نتائج التدقيق

5-4-1 يجب توثيق نتائج جميع المراجعات والتدقيقات الأمنية وتقديم تقارير رسمية للإدارة المختصة.

5-4-2 تحتوي التقارير على نقاط الضعف، مستوى المخاطر، الإجراءات التصحيحية، والمدة الزمنية للمعالجة.

5-5 المعالجة والمتابعة

5-5-1 تلتزم الجهات المعنية بتنفيذ الإجراءات التصحيحية خلال الفترة الزمنية المحددة في تقرير التدقيق.

5-5-2 يتم متابعة التنفيذ من قبل مسؤول الأمن السيبراني لضمان إغلاق الثغرات بشكل صحيح.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد خطة التدقيق، مراجعة التقارير، وتوفير الموارد اللازمة.
مسؤول الأمن السيبراني	إعداد خطط التدقيق، الإشراف على المراجعات، توثيق النتائج، ومتابعة المعالجات.
قسم تقنية المعلومات	دعم عمليات التدقيق، توفير المعلومات المطلوبة، وتنفيذ الإجراءات التصحيحية.
جميع الموظفين	التعاون الكامل أثناء المراجعات وعدم حجب أي معلومات مطلوبة.

الالتزام بالسياسة

- يعد الالتزام بهذه السياسة إلزامياً لجميع الموظفين والإدارات المعنية.
- أي محاولة لتعطيل أو إخفاء نتائج المراجعة أو عدم تنفيذ الإجراءات التصحيحية تُعد مخالفة صريحة موجبة للعقوبة حسب ضوابط ولوائح شركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لمواكبة المستجدات في مجال الأمن السيبراني.

6- سياسة الأمن السيبراني للموارد البشرية

الغرض

تهدف هذه السياسة إلى دمج ممارسات الأمن السيبراني ضمن دورة عمل الموارد البشرية لضمان حماية أصول المعلومات وتقليل المخاطر الناتجة عن التوظيف أو إدارة المستخدمين داخل شركة جادتك. وتشمل السياسة إجراءات ما قبل وأثناء وما بعد توظيف الموظفين للحفاظ على أمن المعلومات.

المرجع: الضابط الأمني رقم 1-9 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع موظفي شركة جادتك الدائمين والمؤقتين والمتعاقدين.
- الجهات الخارجية التي لديها وصول إلى أنظمة شركة جادتك أو معلوماتها.
- عمليات التوظيف، التدريب، الإشراف، وإنهاء خدمات الموظفين.

بنود السياسة

1-6 التوظيف والتعيين

1-1-6 إجراء فحص الخلفية المهنية (عند الاقتضاء) للموظفين قبل التعيين بما يتناسب مع طبيعة الوظيفة.

2-1-6 توقيع الموظفين على اتفاقيات سرية المعلومات وسياسات الاستخدام المقبول.

2-6 التوعية والتدريب

1-2-6 توفير برامج تدريب دورية للموظفين حول الأمن السيبراني والتهديدات الشائعة.

2-2-6 التأكد من فهم الموظفين لدورهم في حماية المعلومات.

3-6 إدارة صلاحيات الوصول

1-3-6 منح صلاحيات الوصول بناءً على مبدأ أقل قدر من الصلاحيات.(Least Privilege)

2-3-6 مراجعة الصلاحيات بشكل دوري للتأكد من مطابقتها لمهام الموظف الحالية.

3-3-6 سحب أو تعديل الصلاحيات فور تغيير الوظيفة أو إنهاء الخدمة.

4-6 السلوك الأمني داخل بيئة العمل

1-4-6 الالتزام باستخدام الأنظمة والأجهزة والتطبيقات الرسمية المعتمدة فقط.

2-4-6 الإبلاغ الفوري عن أي محاولة أو نشاط مشبوه يتعلق بأمن المعلومات.

5-6 إنهاء الخدمة

1-5-6 سحب جميع صلاحيات الوصول وحظر الحسابات فور إنهاء خدمة الموظف.

2-5-6 استرجاع جميع الأجهزة والبيانات والسجلات المتعلقة بشركة جادتك قبل مغادرة الموظف.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة ودعم تطبيقها.
إدارة الموارد البشرية	تنفيذ الفحص قبل التوظيف، توثيق الاتفاقيات، والتنسيق مع الأمن السيبراني بشأن الصلاحيات.
مسؤول الأمن السيبراني	تطوير برامج التوعية، مراجعة الصلاحيات، مراقبة السلوك الأمني.
قسم تقنية المعلومات	تنفيذ عمليات منح/سحب الصلاحيات وضمان تأمين الأجهزة والأنظمة.
الموظفون	الالتزام بسياسات الأمن السيبراني والإبلاغ عن أي مخالفات.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي وجزء من مسؤوليات الموظف الوظيفية.
- أي مخالفة قد تؤدي إلى إجراءات نظامية تشمل الإنذارات أو المساءلة الإدارية وفق لوائح شركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لضمان ملاءمتها للتغيرات والشروط التنظيمية.

7- سياسة الاستخدام المقبول للأصول

الغرض

تهدف هذه السياسة إلى تحديد ضوابط ومعايير الاستخدام الصحيح والمسموح للأصول التقنية الخاصة بشركة جادتك، بما يشمل الأجهزة، الشبكات، البريد الإلكتروني، أنظمة المعلومات، والإنترنت، وذلك لضمان حماية الموارد ومنع إساءة الاستخدام أو التسبب في مخاطر أمنية أو تشغيلية.

المرجع: الضابط الأمني رقم 2-1 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع موظفي شركة جادتك والمتدربين والعاملين بعقود مؤقتة.
- جميع مقدمي الخدمات الخارجيين الذين لديهم وصول إلى أنظمة شركة جادتك أو بياناتها.
- جميع الأصول التقنية مثل الحواسيب، الهواتف، الخوادم، الشبكات، قواعد البيانات، البريد الإلكتروني، والإنترنت.

بنود السياسة

1-7 الاستخدام المصرح به

1-1-7 يُسمح باستخدام الأصول التقنية لأغراض العمل الرسمي فقط.

2-1-7 يمنع استخدام الأصول لقضايا شخصية أو تجارية خارج نطاق مهام الوظيفة.

2-7 البريد الإلكتروني والإنترنت

1-2-7 استخدام البريد الإلكتروني المهني يجب أن يكون لأغراض العمل فقط.

2-2-7 يمنع زيارة المواقع غير الموثوقة أو التي تحتوي على محتوى ضار أو مخالف للأخلاق.

3-7 حماية الحسابات وكلمات المرور

1-3-7 يجب على المستخدمين الحفاظ على سرية كلمات المرور وعدم مشاركتها مع الآخرين.

2-3-7 استخدام كلمات مرور موثوقة وتغييرها بشكل دوري.

4-7 تثبيت البرامج

7-4-1 يمنع تثبيت أي برامج أو أدوات غير معتمدة دون موافقة مسبقة من قسم تقنية المعلومات.

7-4-1 يجب التأكد من مصادر البرامج قبل تحميلها أو استخدامها.

5-7 التعامل مع البيانات

7-5-1 يجب حماية المعلومات الحساسة وعدم مشاركتها إلا مع الأشخاص المخولين.

7-5-2 يمنع نسخ أو نقل بيانات شركة جادتك إلى أجهزة خارجية دون تصريح رسمي.

6-7 الأجهزة المملوكة لشركة جادتك

7-6-1 يجب الحفاظ على الأجهزة في حالة جيدة وعدم التعديل عليها أو استبدال مكوناتها دون موافقة الجهة المختصة.

7-6-2 الإبلاغ فوراً عن فقدان أو سرقة أي جهاز.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
قسم الأمن السيبراني	مراقبة الالتزام بالسياسة وإصدار التوجيهات والتحديثات الدورية.
قسم تقنية المعلومات	إدارة الأصول التقنية، إعداد الضوابط، متابعة صلاحيات المستخدمين، ودعم المستخدمين.
جميع الموظفين	الالتزام باستخدام الأصول وفق السياسة عن أي سوء استخدام أو مخالفة.

الالتزام بالسياسة

- يعد الالتزام بهذه السياسة إلزاميًا لجميع الموظفين والمتعاقدين.
- أي مخالفة أو إساءة استخدام قد تعرض المخالف لإجراءات ادارية أو قانونية.
- تتم مراجعة هذه السياسة بشكل دوري لمواكبة التغييرات التقنية والتهديدات الأمنية.

8- سياسة إدارة هويات الدخول والصلاحيات

الغرض

تهدف هذه السياسة إلى تحديد ضوابط إدارة هويات المستخدمين والصلاحيات داخل الأنظمة والتطبيقات والبنية التحتية التقنية لشركة جادتك، بما يضمن منح الوصول المناسب وفق مبدأ أقل قدر من الصلاحيات (Least Privilege) ، وحماية الأنظمة والمعلومات من الوصول غير المصرح به أو إساءة الاستخدام.

المرجع: الضابط الأمني رقم 2-2 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع الموظفين الدائمين والمؤقتين والمتعاقدين.
- جميع الحسابات التي تصل إلى الأنظمة، التطبيقات، الشبكات، قواعد البيانات، والخدمات السحابية.
- جميع مراحل إدارة الهوية من الإنشاء، التعديل، المتابعة، وتعطيل الحسابات.

بنود السياسة

1-8 إنشاء حسابات المستخدمين

1-1-8 يتم إنشاء الحسابات بناءً على طلب رسمي معتمد من الإدارة المختصة.

2-1-8 يجب ربط كل حساب بمستخدم محدد ولا يُسمح باستخدام الحسابات المشتركة.

2-8 مبدأ أقل قدر من الصلاحيات (Least Privilege)

1-2-8 تُمنح الصلاحيات وفق المهام الوظيفية فقط.

2-2-8 يمنع منح أي صلاحيات إضافية غير ضرورية لأداء مهام العمل.

3-8 إدارة الوصول والصلاحيات

1-3-8 يجب مراجعة الصلاحيات بشكل دوري (على الأقل كل 3 أشهر).

2-3-8 يتم تعديل الصلاحيات فور تغيير مهام الموظف، أو نقله، أو ترقيته.

3-3-8 يتم إيقاف الصلاحيات فورا لأي موظف ترك العمل او تم إيقافه عن العمل.

4-8 تعطيل الحسابات

1-4-8 تُعطل الحسابات فور انتهاء علاقة الموظف بشركة جادتك أو توقف الحاجة لاستخدامها.

2-4-8 يجب حذف أو أرشفة الحسابات غير النشطة بعد مدة محددة يتم تحديدها من قبل الأمن السيبراني.

5-8 المصادقة وكلمات المرور

1-5-8تفعيل المصادقة متعددة العوامل (MFA) على الأنظمة الحرجة والخدمات السحابية.

2-5-8 الالتزام بسياسة كلمات المرور الخاصة بشركة جادتك من حيث التعقيد والتغيير الدوري.

6-8 مراقبة الدخول

1-6-8 تسجيل ومراقبة كافة عمليات الدخول إلى الأنظمة الحرجة.

2-6-8 يتم التحقيق في أي محاولة وصول غير مأذون بها أو مشبوهة فوراً.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
قسم الموارد البشرية	إبلاغ قسم تقنية المعلومات عند توظيف أو نقل أو إنهاء خدمات الموظفين لضبط الصلاحيات.
مسؤول الأمن السيبراني	مراجعة الصلاحيات، متابعة الالتزام، التحقيق في أي خروقات.
قسم تقنية المعلومات	إنشاء، تعديل، وتعطيل الحسابات وإدارة أنظمة المصادقة وفق الإجراءات المعتمدة.
الموظفون	استخدام الحسابات الممنوحة لهم فقط وعدم مشاركة بيانات الدخول مع أي جهة أو فرد.

الالتزام بالسياسة

- الالتزام بهذه السياسة إجباري لجميع الموظفين والجهات ذات العلاقة.
- أي انتهاك أو إساءة استخدام لصلاحيات الدخول يعرض الموظف للمساءلة الإدارية أو القانونية.
- تتم مراجعة هذه السياسة بشكل دوري لمواكبة التحديثات التقنية والتنظيمية.

9- سياسة أمن قواعد البيانات

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات في شركة جادتك لحماية قواعد البيانات من الوصول غير المصرح به، أو فقدان البيانات، أو التعديل غير المصرح به، أو الهجمات السيبرانية، وذلك لضمان سرية وسلامة وتوافر المعلومات المخزنة.

المرجع: الضابط الأمني رقم 2-3 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع قواعد البيانات التي تمتلكها أو تديرها شركة جادتك.
- جميع الموظفين والمتعاقدين الذين لديهم صلاحيات للوصول لقواعد البيانات.
- الأنظمة والتطبيقات والخوادم التي تتفاعل مع قواعد البيانات.
- أي أطراف خارجية تقدم خدمات تتعلق بإدارة أو استضافة قواعد البيانات.

بنود السياسة

9-1 التحكم في الوصول

9-1-1 يجب منح صلاحيات الوصول لقواعد البيانات بناءً على الأدوار الوظيفية فقط.

9-1-2 يمنع استخدام الحسابات المشتركة، ويجب ربط كل حساب بمستخدم محدد.

9-1-3 تفعيل المصادقة متعددة العوامل (MFA) لقواعد البيانات الحرجة.

9-2 تشفير البيانات

9-2-1 يجب تشفير البيانات الحساسة أثناء النقل (In-Transit) والتخزين.(At-Rest)

9-2-2 استخدام بروتوكولات اتصال آمنة مثل TLS/SSL عند ربط الأنظمة بقواعد البيانات.

9-3 إدارة كلمات المرور

9-3-1 تطبيق سياسات كلمات المرور المعتمدة في شركة جادتك لقواعد البيانات.

9-3-2 تغيير كلمات المرور الافتراضية عند تثبيت أنظمة قواعد البيانات الجديدة.

4-9 التحديثات والتصحيحات الأمنية

9-4-1 تثبيت التحديثات الأمنية والتصحيحات الخاصة بقواعد البيانات بانتظام.

9-4-2 اختبار التحديثات في بيئة تجريبية قبل تطبيقها في البيئة الانتاجية.

5-9 النسخ الاحتياطي والاستعادة

9-5-1تنفيذ نسخ احتياطي دوري لقواعد البيانات وفق جدول معتمد.

9-5-2 اختبار خطط استعادة البيانات بصفة دورية لضمان فعاليتها.

6-9 المراقبة والتسجيل (Logging & Monitoring)

9-6-1 تفعيل تسجيل الأحداث والأنشطة التي تتم على قواعد البيانات.

9-6-2 مراجعة السجلات بشكل دوري لاكتشاف الأنشطة غير المصرح بها أو المشبوهة.

7-9 اختبارات الأمن والتدقيق

9-7-1 تنفيذ اختبارات اختراق ومراجعات أمنية لقواعد البيانات بصفة دورية.

9-7-2 معالجة الثغرات التي يتم اكتشافها خلال وقت محدد ومعتمد.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها.
مسؤول الأمن السيبراني	مراقبة الالتزام، وتقييم المخاطر، ومراجعة إعدادات الأمان الخاصة بقواعد البيانات.
قسم تقنية المعلومات / مسؤولو قواعد البيانات(DBA)	تنفيذ إجراءات الحماية، إدارة الصلاحيات، تطبيق النسخ الاحتياطي، ومراقبة السجلات.
الموظفون والمستخدمون	استخدام قواعد البيانات ضمن الصلاحيات المحددة وعدم محاولة تجاوز الضوابط الأمنية.

الالتزام بالسياسة

- يعد الالتزام بهذه السياسة إلزامياً لجميع العاملين في شركة جادتك والجهات ذات الصلة.
- أي مخالفات أو تجاوزات تعتبر انتهاكًا أمنيًا يستوجب اتخاذ إجراءات ادارية أو قانونية.
- يتم مراجعة هذه السياسة بصفة دورية لضمان توافقها مع التطورات التقنية وضوابط الأمن السيبراني.

10- سياسة امن الخادم

الغرض

تهدف هذه السياسة إلى وضع الضوابط والمعايير اللازمة لتأمين الخوادم التي تديرها شركة جادتك وحمايتها من التهديدات الأمنية، وذلك لضمان سرية وسلامة وتوافر البيانات والخدمات التقنية التي تعتمد عليها شركة جادتك.

المرجع: الضابط الأمني رقم 2-3 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- جميع خوادم شركة جادتك (الداخلية، السحابية، الإنتاجية، والاختبارية).
- موظفي تقنية المعلومات ومسؤولي الأنظمة والدعم الفني.
- الخوادم التي تستضيفها جهات خارجية أو مقدمو خدمات سحابية بالنيابة عن شركة جادتك.
- جميع عمليات الإعداد، التشغيل، التحديث، الصيانة، والمراقبة المتعلقة بالخوادم.

بنود السياسة

1-10 إعداد الخوادم وتحصينها

1-1-10 يجب تثبيت الأنظمة والتطبيقات الضرورية فقط على الخوادم.

2-1-10 تعطيل الخدمات والمنافذ غير المستخدمة.

3-1-10 تطبيق سياسات الإعداد الآمن (Secure Configuration Standards) قبل تشغيل الخادم.

2-10 التحديثات والتصحيحات الأمنية

1-2-10 تثبيت التحديثات الأمنية والتصحيحات الخاصة بأنظمة التشغيل والتطبيقات بشكل دوري.

2-2-10 إجراء اختبارات التوافق قبل تطبيق التحديثات في بيئة الإنتاج.

3-10 إدارة الوصول والصلاحيات

1-3-10 منح الصلاحيات بناءً على مبدأ أقل قدر من الصلاحيات (Least Privilege).

10-3-2 تفعيل المصادقة متعددة العوامل (MFA) للوصول إلى خوادم الإنتاج.

10-3-3 حظر استخدام الحسابات الافتراضية أو المشتركة.

10-4 حماية الشبكات والاتصالات

10-4-1 وضع الخوادم ضمن شبكات محمية وجدران نارية مناسبة.

10-4-2 استخدام بروتوكولات اتصال مشفرة مثل SSH وTLS

10-4-3 عزل خوادم الإنتاج عن خوادم الاختبار والتطوير.

10-5المراقبة وتسجيل الأحداث

10-5-1 تفعيل سجل الأحداث (Logs) على الخوادم ومراقبتها بشكل دوري.

10-5-2 الإبلاغ عن أي نشاط مشبوه فور اكتشافه.

10-5-3 الاحتفاظ بسجلات الدخول لفترة زمنية معتمدة.

10-6 النسخ الاحتياطي وخطط الاستعادة

10-6-1 تنفيذ النسخ الاحتياطي للخوادم وفق جداول معتمدة.

10-6-2 اختبار خطط الاستعادة للتأكد من جاهزيتها في حال حدوث أعطال أو هجمات.

10-7 اختبارات الأمن والتدقيق

10-7-1 إجراء مراجعات أمنية واختبارات اختراق دورية للخوادم.

10-7-2 معالجة نقاط الضعف المكتشفة ضمن مدة محددة من قبل الأمن السيبراني.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	الموافقة على السياسة ودعم تنفيذها.
مسؤول الأمن السيبراني	مراقبة الالتزام، تقييم المخاطر، وإصدار التوصيات الأمنية.
قسم تقنية المعلومات / مسؤولو الخوادم	تنفيذ الإعدادات والتحصين، إدارة الوصول، مراقبة الخوادم، وتطبيق النسخ الاحتياطي.
الموظفون والمستخدمون	استخدام الأنظمة وفق الصلاحيات وعدم محاولة الوصول غير المصرح به.

الالتزام بالسياسة

- هذه السياسة إلزامية لجميع الموظفين وأصحاب الصلاحيات الفنية.
- أي مخالفة أو محاولة الوصول غير المصرح به إلى الخوادم قد يؤدي لإجراءات ادارية أو قانونية.
- تتم مراجعة هذه السياسة بشكل دوري لمواكبة تطورات الأمن السيبراني والتقنيات الحديثة.

11- سياسة الحماية من البرمجيات الضارة

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات تساعد في منع البرمجيات الضارة من إصابة أنظمة وأجهزة شركة جادتك، والكشف عنها والاستجابة لها في حال حدوثها، وذلك لضمان حماية بيانات وأصول شركة جادتك والمحافظة على استمرارية الأعمال.

المرجع: الضابط الأمني رقم 2-3 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- أنظمة التشغيل، أجهزة الحاسب المكتبية والمحمولة، الأجهزة الذكية، الخوادم، الشبكات، والتطبيقات التابعة لشركة جادتك.
- الموظفين والمتعاقدين وأي مستخدم لديه حق الوصول إلى أصول شركة جادتك التقنية.
- الملفات، البرامج، الرسائل، والوسائط التي يتم تبادلها أو تحميلها أو تشغيلها ضمن بيئة العمل.

بنود السياسة

1-11 الوقاية من البرمجيات الضارة

1-1-11 تثبيت برامج حماية (Anti-Malware / Endpoint Protection)على الأجهزة والخوادم.

2-1-11 تفعيل التحديث التلقائي لبرامج الحماية وقواعد التعرف على التهديدات.

3-1-11 منع تثبيت أو تشغيل أي ملفات أو برامج من مصادر غير موثوقة.

2-11 مراقبة واكتشاف التهديدات

1-2-11 تفعيل خاصية الفحص الدوري والآلي للأجهزة والشبكات.

2-2-11 مراقبة التنبيهات والسجلات الصادرة من أنظمة الحماية وتحليل الأنشطة المشبوهة.

3-11 الحد من الامتيازات

1-3-11 تطبيق مبدأ أقل قدر من الصلاحيات لمستخدمي الأنظمة لتقليل احتمالية تشغيل البرمجيات الضارة.

11-3-2 منع المستخدمين من تثبيت البرامج دون موافقة قسم تقنية المعلومات.

11-4 البريد الإلكتروني والإنترنت

11-4-1 تفعيل بوابات فحص البريد الإلكتروني للكشف عن الروابط والمرفقات الضارة.

11-4-2 حظر الوصول إلى المواقع المشبوهة أو غير الموثوقة عبر أنظمة تصفية الويب.

11-5 الاستجابة للحوادث

11-5-1 في حالة اكتشاف برمجية ضارة، يجب عزل الجهاز المصاب فورًا وإبلاغ فريق الأمن السيبراني.

11-5-1 توثيق الحادث، تحليل السبب الجذري، واتخاذ إجراءات تصحيحية لمنع التكرار.

11-6 التوعية والتدريب

11-6-1 تنفيذ برامج توعية دورية حول البرمجيات الضارة وطرق اكتشافها والتعامل معها.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الدعم والموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	مراقبة تنفيذ السياسة، تحليل التهديدات، والاستجابة للحوادث.
قسم تقنية المعلومات	تثبيت برامج الحماية، والمراقبة ، والفحص الدوري، ومعالجة الإصابات.
جميع الموظفين	الالتزام بالإجراءات الأمنية، وعدم تثبيت برامج غير معتمدة، والإبلاغ عن الحوادث فورًا.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي على جميع المستخدمين.
- أي مخالفة قد تؤدي إلى إجراءات إدارية، وقد تصل للعقوبات النظامية عند الضرورة.
- تتم مراجعة هذه السياسة بشكل دوري لتحديثها وفق أحدث التهديدات والمتطلبات التنظيمية.

12- سياسة حزم التحديثات والاصلاحات

الغرض

تهدف هذه السياسة إلى حماية أنظمة شركة جادتك وشبكاتها من التهديدات والثغرات الأمنية عن طريق إدارة فعّالة للتحديثات والإصلاحات. كما تهدف إلى ضمان تطبيق التحديثات بطريقة منظمة، تقلل المخاطر، وتحافظ على استمرارية الأعمال وموثوقية الأنظمة.

المرجع: الضابط الأمني رقم 2-3 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- أجهزة الحواسيب المكتبية والمحمولة، الخوادم، الشبكات، وأنظمة التشغيل والتطبيقات داخل بيئة شركة جادتك.
- الأنظمة الداخلية والخدمات السحابية المعتمدة من قبل شركة جادتك.
- الموظفين والفريق التقني المسؤول عن إدارة وصيانة الأنظمة.

بنود السياسة

12-1 تقييم التحديثات

12-1-1 تقييم كل تحديث أو إصلاح لتحديد أهميته، مستوى المخاطر، وتأثيره على الأنظمة.

12-2 تصنيف التحديثات

12-2-1 حرجة (Critical) تحديثات أمنية لإصلاح ثغرات تهدد سلامة الأنظمة.

12-2-2 مهمة (Important) تحسين الأداء أو معالجة مشكلات رئيسية.

12-2-3 اختيارية (Optional) تحسينات إضافية أو مزايا غير أساسية.

12-3 اختبار التحديثات

12-3-1 اختبار التحديثات على بيئة تجريبية قبل تطبيقها على البيئة الإنتاجية لتجنب أي تأثير سلبي.

12-4 جدولة التحديثات

12-4-1 تطبيق التحديثات وفق جدول زمني محدد يضمن الحد الأدنى من تأثيرها على سير الأعمال.

5-12 توثيق التحديثات

1-5-12 تسجيل جميع التحديثات المطبقة، بما في ذلك التاريخ، الأجهزة المستهدفة، وحالة التطبيق.

6-12 النسخ الاحتياطي

1-6-12 تنفيذ نسخة احتياطية للأنظمة الحرجة قبل تطبيق أي تحديثات رئيسية أو حرجة.

7-12 التعامل مع التحديثات غير الآمنة

1-7-12 أي تحديثات تسببت بمشكلات أو ثغرات يجب التعامل معها فوراً واتخاذ الإجراءات المناسبة.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
قسم تكنولوجيا المعلومات / الفريق التقني	تقييم، اختبار، تطبيق وتوثيق جميع التحديثات.
مسؤول الأمن السيبراني	مراجعة سياسة التحديثات وضمان توافقها مع متطلبات الأمن السيبراني لشركة جادتك.
مدير الأنظمة والشبكات	متابعة تطبيق التحديثات على الأجهزة والخوادم وضمان الالتزام بالجدول الزمني.
الموظفون	التعاون مع الفريق التقني وعدم تعطيل عمليات التحديث على أجهزتهم.

الالتزام بالسياسة

- جميع الموظفين والفريق التقني ملزمون بالامتثال لهذه السياسة لضمان حماية أنظمة شركة جادتك.
- أي خرق لهذه السياسة سيخضع لإجراءات ادارية وفق نظام شركة جادتك.
- يتم مراجعة السياسة بشكل دوري لضمان مواكبتها لأحدث التهديدات الأمنية والمتطلبات التنظيمية.

13- سياسة امن وسائط التخزين

الغرض

تهدف هذه السياسة إلى حماية وسائط التخزين (مثل الأقراص الصلبة، USB، أجهزة التخزين المحمولة، وسائط النسخ الاحتياطي) من الوصول غير المصرح به، الفقدان، السرقة، أو التلف. كما تهدف لضمان الحفاظ على سرية وسلامة البيانات المخزنة عليها وتجنب أي تهديد للأمن السيبراني لشركة جادتك.

المرجع: الضابط الأمني رقم 2-3 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- وسائط التخزين الداخلية والخارجية المستخدمة داخل بيئة شركة جادتك.
- البيانات المخزنة على وسائط التخزين سواء كانت حساسة أو عامة.
- الموظفين والفريق التقني المسؤول عن استخدام، نقل، أو إدارة وسائط التخزين.

بنود السياسة

13-1 تصنيف الوسائط

13-1-1 يجب تصنيف جميع وسائط التخزين حسب نوع البيانات المخزنة عليها (حساسة، داخلية، عامة).

13-2 التشفير

13-2-1 يجب تشفير جميع البيانات المخزنة على وسائط قابلة للإزالة أو خارجية لتجنب الوصول غير المصرح به.

13-3 الوصول والتحكم

13-3-1 منح الوصول إلى وسائط التخزين حسب الحاجة الوظيفية فقط.

13-4 التخزين الآمن

13-4-1 تخزين وسائط التخزين في أماكن محمية، مقفلة، وبعيدة عن العوامل البيئية الضارة.

13-5 النقل

13-5-1 عند نقل وسائط التخزين خارج شركة جادتك، يجب الالتزام بطرق النقل الآمنة والتشفير الكامل للبيانات.

13-6 النسخ الاحتياطي

13-6-1 يجب ضمان وجود نسخ احتياطية من البيانات المخزنة على وسائط التخزين الهامة، وتخزينها بطريقة آمنة.

13-7 التدقيق والمراجعة

13-7-1 إجراء مراجعات دورية للوسائط المخزنة وتوثيق عمليات الوصول والاستخدام.

13-8 التخلص الآمن

13-8-1 يجب التخلص من وسائط التخزين المحتوية على بيانات حساسة بطريقة تمنع استرجاعها، مثل التدمير الفيزيائي أو المحو الآمن للبيانات.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الفريق التقني / قسم تكنولوجيا المعلومات	إدارة وسائط التخزين، تشفير البيانات، النسخ الاحتياطي، وضمان الامتثال للسياسة.
مسؤول الأمن السيبراني	مراجعة السياسات، متابعة تنفيذها، وضمان حماية البيانات الحساسة.
الموظفون	الالتزام بالتعامل الآمن مع وسائط التخزين، عدم مشاركة وسائط التخزين مع أطراف غير مصرح لها، والإبلاغ عن أي فقدان أو سرقة.
إدارة شركة جادتك	دعم وتنفيذ السياسات، توفير الموارد اللازمة لتطبيق الإجراءات الأمنية.

الالتزام بالسياسة

- جميع الموظفين والفريق التقني ملزمون بالالتزام بهذه السياسة لضمان حماية البيانات المخزنة على وسائط التخزين.
- أي خرق للسياسة سيخضع لإجراءات ادارية وفق نظام شركة جادتك.
- تُراجع هذه السياسة بشكل دوري لضمان مواكبتها لأحدث التهديدات الأمنية والمتطلبات التنظيمية.

14- سياسة امن البريد الإلكتروني

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات لحماية البريد الإلكتروني لشركة جادتك من التهديدات الإلكترونية مثل التصيد الاحتيالي، البرمجيات الضارة، وتسريب المعلومات، وضمان استخدام البريد الإلكتروني بطريقة آمنة تتوافق مع متطلبات الأمن السيبراني وحماية بيانات شركة جادتك.

المرجع: الضابط الأمني رقم 2-4 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- حسابات البريد الإلكتروني الرسمية التابعة لشركة جادتك.
- الموظفين والمتعاقدين وأي مستخدم لديه حق الوصول إلى البريد الإلكتروني لشركة جادتك.
- الرسائل المرسلة والمستلمة، والمرفقات، والروابط المرتبطة بالبريد الإلكتروني ضمن بيئة العمل.

بنود السياسة

1-14 التحكم بالوصول

1-1-14 استخدام كلمات مرور موثوقة ومعقدة لجميع حسابات البريد الإلكتروني.

2-1-14 تفعيل المصادقة متعددة العوامل (MFA) لحماية الحسابات.

3-1-14 منع مشاركة بيانات الدخول أو الحسابات مع أي جهة غير مصرح لها.

2-14 الوقاية من التهديدات

1-2-14 تفعيل فلترة البريد الإلكتروني للكشف عن الرسائل الاحتيالية والمرفقات الضارة.

2-2-14 حظر الرسائل التي تحتوي على روابط أو ملفات مشبوهة قبل وصولها للمستخدم.

3-2-14 تحديث أنظمة الحماية من البريد الإلكتروني بشكل دوري لضمان اكتشاف أحدث التهديدات.

3-14 الاستخدام الآمن للبريد الإلكتروني

1-3-14 عدم فتح الروابط أو المرفقات من مصادر غير موثوقة.

2-3-14 الامتناع عن إرسال المعلومات الحساسة عبر البريد الإلكتروني إلا إذا كانت مشفرة.

3-3-14 استخدام البريد الإلكتروني الرسمي فقط للأغراض المهنية.

4-14 الاستجابة للحوادث

1-4-14 الإبلاغ فوراً عن أي رسالة مشبوهة أو محتوى ضار إلى فريق الأمن السيبراني.

2-4-14 عزل أي حسابات مخترقة واتخاذ إجراءات تصحيحية فورية.

3-4-14 توثيق أي حادثة بريد إلكتروني وتحليل السبب الجذري لمنع تكرارها.

5-14 التوعية والتدريب

1-5-14 تقديم برامج توعية دورية للموظفين حول تهديدات البريد الإلكتروني وأفضل الممارسات للتعامل معها.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الدعم والموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	مراقبة تنفيذ السياسة، تحليل التهديدات، والاستجابة للحوادث البريدية.
قسم تقنية المعلومات	إدارة حسابات البريد الإلكتروني، تفعيل الحماية، مراقبة الرسائل المشبوهة، وتنفيذ الإجراءات التصحيحية.
جميع الموظفين	الالتزام بالإجراءات الأمنية، عدم فتح الرسائل المشبوهة، الإبلاغ عن أي حوادث.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي على جميع مستخدمي البريد الإلكتروني لشركة جادتك.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات إدارية ، وقد تصل إلى العقوبات النظامية عند الضرورة.
- تتم مراجعة هذه السياسة بشكل دوري لضمان مواكبتها لأحدث التهديدات والمتطلبات التنظيمية.

15- سياسة امن الشبكات

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات لحماية شبكات شركة جادتك من الوصول غير المصرح به، والهجمات السيبرانية، والتسريب أو العبث بالبيانات، وذلك لضمان استمرارية الأعمال، وسلامة المعلومات، وموثوقية البنية التحتية التقنية.

المرجع: الضابط الأمني رقم 2-5 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- مكونات الشبكة بما في ذلك الأجهزة، الخوادم، الراوترات، السويتشات، الجدران النارية، الشبكات السلكية واللاسلكية.
- الموظفين، المتعاقدين، ومقدمي الخدمات الذين لديهم حق الوصول إلى شبكة شركة جادتك.
- عمليات الاتصال، نقل البيانات، إدارة الشبكات، والدخول إلى الأنظمة عبر الشبكة.

بنود السياسة

1-15 التحكم بالوصول إلى الشبكة

1-1-15 السماح بالوصول للشبكة فقط للمستخدمين والأجهزة المصرح بها.

2-1-15 تطبيق المصادقة المتقدمة (MFA / 802.1X) حيثما أمكن.

3-1-15 استخدام شبكات منفصلة للأجهزة الشخصية والزوار عن الشبكة الداخلية لشركة جادتك.

2-15 الجدران النارية والأنظمة الأمنية

1-2-15 استخدام جدار ناري (Firewall) لحماية الشبكة الداخلية من التهديدات الخارجية.

2-2-15 تفعيل أنظمة كشف ومنع التسلل (IDS/IPS) ومراقبة الأنشطة المشبوهة.

3-2-15 تحديث توقيعات وقواعد الحماية بشكل دوري.

3-15 إدارة الشبكات والتكوين

1-3-15 تطبيق معيار موحد لإعداد وتكوين أجهزة الشبكة لضمان الأمان.

15-3-2 عدم استخدام الإعدادات الافتراضية لكلمات المرور أو المنافذ المفتوحة.

15-3-3 إجراء مراجعات دورية لإعدادات الشبكات وتوثيق أي تغييرات.

15-4 أمن الشبكات اللاسلكية

15-4-1 تشفير الشبكة اللاسلكية باستخدام بروتوكولات تشفير موثوقة مثل WPA3 أو ما يعادله.

15-4-2 عدم بث الشبكات الداخلية للعامة.

15-4-3 توفير شبكة منفصلة ومحدودة للزوار عند الضرورة.

15-5 المراقبة والتسجيل

15-5-1 مراقبة حركة الشبكة والأنشطة بشكل مستمر.

15-5-2 تسجيل الأحداث في أنظمة الشبكة والاحتفاظ بالسجلات لفترة مناسبة للتحليل والمراجعة.

15-6 الاستجابة للحوادث

15-6-1 الإبلاغ الفوري عن أي نشاط غير اعتيادي أو اختراق للشبكة لفريق الأمن السيبراني.

15-6-2 عزل العناصر المصابة والتحقق من مصدر الهجوم واتخاذ الإجراءات التصحيحية.

15-6-3 توثيق الحادث وتحليل أسبابه لمنع تكراره مستقبلاً.

15-7 التوعية

15-7-1 تنفيذ برامج تدريب دورية للعاملين حول الاستخدام الآمن للشبكات ومخاطر الإهمال الأمني.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على تنفيذ السياسة، مراقبة التهديدات، والاستجابة للحوادث.
قسم تقنية المعلومات / فريق الشبكات	إدارة إعدادات الشبكة، تطبيق ضوابط الحماية، مراقبة الأنشطة، وتنفيذ الصيانة الدورية.
جميع الموظفين	الالتزام باستخدام الشبكة بطريقة آمنة والإبلاغ عن أي أنشطة مريبة.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع مستخدمي شبكة شركة جادتك.
- أي مخالفة لهذه السياسة قد تؤدي إلى إجراءات إدارية أو قانونية عند الضرورة.
- تتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع أحدث التهديدات والتقنيات والمعايير التنظيمية.

16- سياسة امن أجهزة المستخدمين والأجهزة المحمولة والشخصية

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات لحماية أجهزة المستخدمين وأجهزة الاتصال المحمولة والشخصية المستخدمة في الوصول إلى موارد وأنظمة شركة جادتك، وذلك للحد من المخاطر الأمنية، حماية البيانات السرّية، وضمان استمرارية الأعمال من خلال منع الاختراقات والتسريب أو العبث بالمعلومات.

المرجع: الضابط الأمني رقم 2-6 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- أجهزة الحاسب المكتبية والمحمولة التابعة لشركة جادتك.
- الأجهزة الذكية وأجهزة الهواتف المحمولة والأجهزة اللوحية المستخدمة لأغراض العمل.
- الأجهزة الشخصية المسموح لها بالاتصال بشبكة أو أنظمة شركة جادتك وفق ضوابط العمل.(BYOD)
- الموظفين والمتعاقدين والمستخدمين الذين لديهم حق الوصول إلى أصول وأنظمة شركة جادتك عبر هذه الأجهزة.

بنود السياسة

1-16 الحماية والتكوين

1-1-16 تثبيت برامج الحماية المعتمدة (Antivirus / Endpoint Security) على جميع الأجهزة.

2-1-16 تفعيل التحديثات التلقائية لنظام التشغيل وبرامج الحماية.

3-1-16 تطبيق كلمات مرور موثوقة أو وسائل حماية بيومترية على جميع الأجهزة.

4-1-16 قفل الشاشة تلقائياً بعد فترة محددة من عدم الاستخدام.

2-16 التحكم في الوصول

1-2-16 يسمح بالوصول إلى بيانات وأنظمة شركة جادتك فقط عبر حسابات مصرح بها.

2-2-16 يحظر مشاركة كلمات المرور أو بيانات الدخول مع أي طرف آخر.

3-2-16 تفعيل المصادقة متعددة العوامل (MFA) عند الوصول إلى الأنظمة الحساسة.

3-16 الأجهزة الشخصية(BYOD)

1-3-16 يجب تسجيل الجهاز الشخصي قبل استخدامه في بيئة العمل.

2-3-16 تطبق على الأجهزة الشخصية نفس ضوابط الأمان المطبقة على أجهزة شركة جادتك.

3-3-16 في حال فقدان الجهاز أو سرقته، يحق لفريق الأمن السيبراني مسح بيانات العمل عن بُعد.

4-16 حماية البيانات

1-4-16 يمنع تخزين البيانات الحساسة أو السرّية على الأجهزة دون تشفير.

2-4-16 استخدام شبكات VPN عند الاتصال عن بعد بأنظمة شركة جادتك.

3-4-16 يمنع نقل البيانات عبر وسائط تخزين خارجية ما لم تكن مشفّرة ومعتمدة.

5-16 الاستجابة للحوادث

1-5-16 الإبلاغ فورًا عن أي نشاط غير معتاد، اختراق، فقدان أو سرقة جهاز.

2-5-16 عزل الجهاز المصاب أو المشتبه به عن الشبكة لتقليل الأضرار.

3-5-16 يتم إجراء تحليل للحادث واتخاذ إجراءات تصحيحية لمنع تكراره.

6-16 التوعية والتدريب

1-6-16 تنفيذ جلسات تدريب دورية للمستخدمين حول مخاطر الأجهزة غير الآمنة وكيفية التعامل الآمن معها.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على تنفيذ السياسة، ومراقبة الامتثال، والاستجابة للحوادث.
قسم تقنية المعلومات	إدارة إعدادات الأجهزة، تطبيق حلول الحماية، وتقديم الدعم الفني للمستخدمين.
جميع الموظفين	الالتزام بالإجراءات الأمنية المعتمدة عند استخدام الأجهزة والإبلاغ عن أي حادث فوراً.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع مستخدمي أجهزة شركة جادتك أو الأجهزة الشخصية المتصلة بأنظمتها.
- قد يؤدي عدم الالتزام إلى إجراءات ادارية، وقد تشمل فصل الجهاز عن الشبكة أو اتخاذ إجراءات قانونية عند الحاجة.
- تتم مراجعة هذه السياسة بشكل دوري لضمان مواكبتها لأحدث التهديدات والمعايير التنظيمية.

17- سياسة الامن السيبراني للبيانات

الغرض

تهدف هذه السياسة إلى حماية بيانات شركة جادتك من الوصول غير المصرح به، التعديل، التسريب، الفقدان أو التدمير، وضمان سرية البيانات وسلامتها وتوفرها، وذلك من خلال وضع ضوابط ومعايير تحكم إدارة البيانات في جميع مراحلها داخل بيئة العمل.

المرجع: الضابط الأمني رقم 2-7 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- البيانات التي تمتلكها أو تديرها شركة جادتك، سواء كانت مخزنة أو منقولة أو قيد المعالجة.
- مستخدمي الأنظمة التقنية، بما في ذلك الموظفين، المتعاقدين، ومقدمي الخدمات.
- أنظمة المعلومات، الخوادم، قواعد البيانات، أجهزة الحاسب، وسائط التخزين، والحلول السحابية المستخدمة في التعامل مع البيانات.

بنود السياسة

1-17 تصنيف البيانات

1-1-17 يجب تصنيف البيانات وفق مستوى حساسيتها (سرية للغاية، سرية، مقيد، عامة).

2-1-17 يتم تحديد ضوابط الحماية بحسب مستوى التصنيف لتقليل مخاطر الوصول غير المصرح به.

2-17 التحكم في الوصول إلى البيانات

1-2-17 لا يسمح بالوصول إلى البيانات إلا للمستخدمين المصرح لهم وبحسب الحاجة الوظيفية.

2-2-17 تفعيل المصادقة متعددة العوامل (MFA) عند الوصول إلى البيانات الحساسة.

3-2-17 يمنع مشاركة الحسابات أو كلمات المرور بين الأفراد.

3-17 حماية وسلامة البيانات

1-3-17 تشفير البيانات الحساسة أثناء التخزين والنقل.

2-3-17 الالتزام بسياسات النسخ الاحتياطي واستعادة البيانات لضمان استمرارية الأعمال.

3-3-17 منع تعديل أو حذف البيانات بدون صلاحية مسبقة وبما يتوافق مع إجراءات العمل.

4-17 تخزين ونقل البيانات

1-4-17 تخزين البيانات في مواقع وأنظمة معتمدة فقط.

2-4-17 يمنع نقل البيانات الحساسة عبر القنوات غير المشفرة أو التطبيقات غير المرخصة.

3-4-17 عند استخدام خدمات سحابية يجب التأكد من توافقها مع معايير أمن المعلومات.

5-17 مشاركة البيانات

1-5-17 مشاركة البيانات فقط مع جهات أو أفراد مخولين ووفق عقود وسياسات معتمدة.

2-5-17 عدم إرسال البيانات الحساسة عبر البريد الإلكتروني دون تشفير مناسب.

6-17 الاستجابة للحوادث

1-6-17 الإبلاغ الفوري عن أي خرق أو فقدان أو تسريب للبيانات إلى فريق الأمن السيبراني.

2-6-17 توثيق الحادث، وتحليل السبب الجذري، واتخاذ إجراءات تصحيحية لمنع تكراره.

7-17 التوعية والتدريب

1-7-17 تنفيذ برامج توعية دورية لجميع الموظفين حول حماية البيانات وكيفية التعامل معها بشكل آمن.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الدعم والموارد لتنفيذها.
مسؤول الأمن السيبراني	مراقبة الامتثال للسياسة، تحليل المخاطر، والاستجابة لحوادث البيانات.
قسم تقنية المعلومات	إدارة أنظمة البيانات، تطبيق ضوابط الحماية، تنفيذ النسخ الاحتياطي والمعالجة التقنية.
جميع الموظفين	الالتزام بضوابط حماية البيانات، وعدم مشاركة المعلومات الحساسة، والإبلاغ عن أي حادث أمني.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع المستخدمين الذين يتعاملون مع بيانات شركة جادتك.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات إدارية وقد تصل إلى الإجراءات القانونية.
- تتم مراجعة هذه السياسة بشكل دوري لتحديثها وفق أحدث الممارسات والمتطلبات التنظيمية والأمنية.

18- سياسة التشفير

الغرض

تهدف هذه السياسة إلى تحديد الضوابط والمعايير اللازمة لاستخدام تقنيات التشفير لحماية البيانات الحساسة أثناء التخزين أو النقل، وذلك لضمان الحفاظ على سرية وسلامة البيانات ومنع الوصول غير المصرح به في شركة جادتك، بما يساهم في تعزيز الأمن السيبراني ضمن بيئة العمل.

المرجع: الضابط الأمني رقم 2-8 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- البيانات الحساسة أو السرية التي تمتلكها أو تديرها شركة جادتك.
- أنظمة المعلومات، الأجهزة، الخوادم، وسائط التخزين، وقنوات الاتصال التي تتعامل مع بيانات شركة جادتك.
- الموظفين والمتعاقدين والمستخدمين الذين لديهم حق الوصول للبيانات أو يقومون بنقلها أو حفظها.

بنود السياسة

1-18 استخدام التشفير

1-1-18 يجب تشفير البيانات الحساسة أثناء التخزين باستخدام خوارزميات معتمدة.

2-1-18 يجب تشفير البيانات أثناء النقل باستخدام بروتوكولات آمنة مثل (TLS / VPN).

3-1-18 يمنع تخزين البيانات الحساسة على أجهزة أو وسائط تخزين غير مشفرة.

2-18 خوارزميات ومعايير التشفير

1-2-18 يجب استخدام خوارزميات موثوقة ومعتمدة مثل:

AES 256 لتشفير البيانات.

RSA للمفاتيح العامة والخاصة.

SHA-256 أو أعلى للتجزئة.

2-2-18 يمنع استخدام خوارزميات ضعيفة أو غير آمنة مثل : DES وMD5

18-3 إدارة مفاتيح التشفير

18-3-1 يجب إنشاء مفاتيح التشفير وتخزينها وإدارتها بشكل آمن في أنظمة إدارة مفاتيح معتمدة.

18-3-2 يمنع مشاركة مفاتيح التشفير بين الأفراد أو إرسالها عبر قنوات غير آمنة.

18-3-3 يجب استبدال المفاتيح بشكل دوري أو عند الاشتباه بأي اختراق.

18-4 الأجهزة ووسائط التخزين

18-4-1 يجب تشفير الأقراص الصلبة في الأجهزة المحمولة والأجهزة المستخدمة للعمل.

18-4-2 عند التخلص من وسائط تخزين مشفرة، يجب إتلاف المفاتيح المرتبطة بها بشكل يمنع استعادتها.

18-5 الأنظمة السحابية والخدمات الخارجية

18-5-1 يجب التأكد من أن مزودي الخدمات السحابية يدعمون التشفير وفق معايير أمنية معتمدة.

18-5-2 يمنع رفع البيانات الحساسة إلى منصات لا توفر حماية أو إدارة سليمة لمفاتيح التشفير.

18-6 الاستجابة للحوادث

18-6-1 عند الاشتباه بفقدان مفاتيح التشفير أو اختراقها يجب الإبلاغ فوراً لقسم الأمن السيبراني.

18-6-2 يجب استبدال المفاتيح المخترقة واتخاذ إجراء تصحيحي لمنع تكرار الحادث.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	مراقبة تطبيق السياسة، مراجعة مستويات التشفير، والاستجابة للحوادث.
قسم تقنية المعلومات	تنفيذ حلول التشفير، إدارة مفاتيح التشفير، ودعم المستخدمين.
جميع الموظفين	الالتزام بضوابط التشفير وعدم مشاركة المفاتيح أو البيانات بطرق غير آمنة.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع مستخدمي بيانات وأنظمة شركة جادتك.
- أي مخالفة لهذه السياسة قد تؤدي إلى إجراءات ادارية أو قانونية.
- تتم مراجعة السياسة بشكل دوري لتحديثها وفق المستجدات التقنية والمتطلبات الأمنية.

19- سياسة النسخ الاحتياطي

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات النسخ الاحتياطي للبيانات والأنظمة لضمان حماية معلومات شركة جادتك من الفقد أو التلف، وضمان إمكانية استعادة البيانات في حال وقوع حوادث تقنية أو كوارث، مما يعزز استمرارية الأعمال والجاهزية التشغيلية.

المرجع: الضابط الأمني رقم 2-9 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- البيانات والأنظمة والتطبيقات وقواعد البيانات والملفات الإلكترونية الخاصة بشركة جادتك.
- خوادم الإنتاج، الأجهزة المكتبية والمحمولة، والأجهزة المستخدمة في العمل.
- الموظفين والمتعاقدين الذين لديهم حق الوصول إلى بيانات شركة جادتك أو مسؤولية عن تشغيل الأنظمة.

بنود السياسة

1-19 بيانات النسخ الاحتياطي

1-1-19 يجب تحديد البيانات والأنظمة التي تتطلب النسخ الاحتياطي بناءً على أهميتها وحساسيتها.

2-1-19 يجب التأكد من شمول النسخ الاحتياطي لجميع البيانات الحيوية والبيانات التشغيلية المهمة.

2-19 جدول النسخ الاحتياطي

1-2-19 يتم تنفيذ نسخ احتياطي يومي للبيانات الحيوية.

2-2-19يتم تنفيذ نسخ احتياطي أسبوعي لكامل الأنظمة.

3-2-19 يتم الاحتفاظ بنسخ بعيدة الموقع (Off-site / Cloud) لضمان استمرارية الأعمال عند وقوع كوارث.

19-2-4 يتم تنفيذ عملية نسخ احتياطي مجدولة في نهاية يوم العمل الأسبوعي (يوم الخميس الساعة 14:00). ويجب خلال فترة تنفيذ النسخ الاحتياطي إيقاف استخدام الأنظمة والتطبيقات ذات العلاقة، ومنع أي عمليات إدخال أو تعديل أو معالجة بيانات عليها، وذلك لضمان سلامة البيانات واتساقها وعدم تأثر عملية النسخ الاحتياطي.

19-2-5 يتولى قسم تقنية المعلومات مسؤولية إشعار المستخدمين مسبقًا بموعد النسخ الاحتياطي، والتأكد من تطبيق الإيقاف المؤقت للأنظمة، ومراقبة الالتزام بذلك.

19-3 حماية النسخ الاحتياطية

19-3-1 يجب تشفير النسخ الاحتياطية أثناء النقل والتخزين.

19-3-2 يجب تقييد الوصول إلى النسخ الاحتياطية وحفظها في مواقع أو أنظمة آمنة.

19-3-3 يمنع تخزين النسخ الاحتياطية على وسائط غير مؤمنة أو مجهولة المصدر.

19-4 اختبارات الاستعادة

19-4-1 يجب اختبار استعادة البيانات بشكل دوري للتأكد من سلامة النسخ الاحتياطية وقابليتها للاستخدام.

19-4-2 يتم توثيق نتائج الاختبار ومعالجة أي مشكلات تظهر أثناء الاستعادة.

19-5 الإجراءات عند الحوادث

19-5-1 في حال حدوث فقد أو تلف للبيانات، يجب التواصل فوراً مع فريق تقنية المعلومات لبدء إجراءات الاستعادة.

19-5-2 يتم توثيق الحادث وتحليل السبب ومعالجة نقاط الضعف لمنع تكرارها.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد المطلوبة لتنفيذها.
مسؤول الأمن السيبراني	مراقبة تنفيذ النسخ الاحتياطي وضمان سلامة إجراءات الاستعادة.

الجهة / الشخص	المسؤوليات
قسم تقنية المعلومات	تنفيذ عمليات النسخ الاحتياطي، إدارة التخزين، اختبار الاستعادة، وتوثيق العمليات.
جميع الموظفين	حفظ الملفات في المواقع المعتمدة وعدم تخزين البيانات الحساسة خارج الأنظمة الرسمية.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع المستخدمين والجهات ذات العلاقة داخل شركة جادتك.
- أي مخالفة أو إهمال قد يؤدي إلى إجراءات ادارية أو قانونية وفق أنظمة شركة جادتك.
- تتم مراجعة وتحديث هذه السياسة بشكل دوري بما يتناسب مع المستجدات التشغيلية والمتطلبات الأمنية.

20- سياسة إدارة الثغرات

الغرض

تهدف هذه السياسة إلى وضع إطار منهجي لتحديد الثغرات الأمنية في أنظمة شركة جادتك وبيئتها التقنية وتقييمها ومعالجتها في الوقت المناسب، وذلك لتقليل مخاطر الاستغلال وتعزيز حماية البيانات والأصول التقنية واستمرارية العمل.

المرجع: الضابط الأمني رقم 2-10 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- الأجهزة، الخوادم، التطبيقات، قواعد البيانات، الشبكات، ومكونات البنية التحتية التقنية التابعة لشركة جادتك.
- الأنظمة والخدمات الداخلية والخارجية التي يتم استخدامها أو تشغيلها أو إدارتها داخل شركة جادتك أو من قبل أطراف خارجية.
- الموظفين والمتعاقدين الذين لديهم دور في تشغيل أو صيانة الأنظمة التقنية أو التعامل مع بيانات شركة جادتك.

بنود السياسة

1-20 تحديد الثغرات

20-1-1 يتم استخدام أدوات معتمدة لفحص الثغرات بشكل دوري على الأنظمة والأجهزة والشبكات.

20-1-2 يجب تتبع الإعلانات الأمنية الصادرة من الشركات المصنعة والجهات المختصة للتعرف على الثغرات الجديدة.

نوع الاصول	الانظمة					
	جميع الانظمة	الأنظمة الحساسة المتصلة بالإنترنت	الأنظمة الحساسة الداخلية	أنظمة العمل عن بعد	أنظمة حسابات التواصل الاجتماعي	أنظمة خدمات الحوسبة السحابية
أنظمة التشغيل	شهريا	شهريا	شهريا	شهريا	شهريا	شهريا
قواعد البيانات	ثلاث أشهر	شهريا	*ثلاث أشهر	شهريا	شهريا	ثلاث أشهر
أجهزة الشبكة	ثلاث أشهر	شهريا	*ثلاث أشهر	شهريا	شهريا	ثلاث أشهر
التطبيقات	ثلاث أشهر	شهريا	*ثلاث أشهر	شهريا	شهريا	ثلاث أشهر

* يكون فحص الثغرات شهريا بينما يكون تقييم الثغرات كل ثلاث أشهر.

20-2 تقييم وتصنيف الثغرات

20-2-1 يتم تصنيف الثغرات بناءً على مدى خطورتها وتأثيرها على الأنظمة والبيانات (حرجة، عالية، متوسطة، منخفضة).

20-2-2 يجب إعطاء الأولوية في المعالجة للثغرات الحرجة والعالية التي قد تؤثر على سرية أو سلامة أو توفر البيانات.

20-3 معالجة الثغرات

20-3-1 يجب تطبيق إجراءات التصحيح وإصلاح الثغرات وفق جدول زمني معتمد حسب مستوى الخطورة.

20-3-2 يمنع تأجيل إصلاح الثغرات الحرجة إلا بموافقة مكتوبة مبنية على تحليل المخاطر وتدابير تعويضية بديلة.

3-3-20 يجب التأكد من اختبار التحديثات قبل تطبيقها على الأنظمة الإنتاجية لتجنب توقف العمل.

4-20 متابعة وتحسين

1-4-20 يتم توثيق نتائج الفحص والإصلاحات والإجراءات المتخذة لكل ثغرة مكتشفة.

2-4-20 يتم مراجعة إجراءات إدارة الثغرات بشكل دوري وتحسينها بناءً على التجارب والحوادث السابقة.

5-20 التوعية والتدريب

1-5-20 يجب تنفيذ برامج توعية دورية للموظفين حول ممارسات الأمن السيبراني الأساسية التي تقلل فرص الاستغلال.

2-5-20 يجب تدريب مسؤولي الأنظمة على كيفية التعامل مع الثغرات وتحديث الأنظمة بطريقة آمنة.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها.
مسؤول الأمن السيبراني	مراقبة تنفيذ السياسة، تقييم المخاطر، والمتابعة مع الجهات الفنية لمعالجة الثغرات.
قسم تقنية المعلومات	إجراء فحص الثغرات، تطبيق الإصلاحات والتحديثات، وتوثيق الإجراءات المتخذة.
جميع الموظفين	الالتزام بعدم تثبيت برمجيات غير معتمدة، والإبلاغ عن أي سلوك أو مشكلة تقنية مشبوهة.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي على جميع موظفي شركة جادتك والمتعاقدين معها.
- أي مخالفة عمدية أو إهمال قد يؤدي إلى إجراءات ادارية أو قانونية وفق لوائح شركة جادتك.

- يتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع أحدث التهديدات والمتطلبات الأمنية.

21- سياسة اختبار الاختراق

الغرض

تهدف هذه السياسة إلى تحديد الإطار والضوابط اللازمة لتنفيذ اختبارات الاختراق على أنظمة شركة جادتك وتطبيقاتها وبنيتها التحتية، بهدف كشف نقاط الضعف الأمنية قبل استغلالها من قبل جهات خبيثة، وتقييم فعالية ضوابط الأمان، والتأكد من جاهزية أنظمة شركة جادتك لمواجهة الهجمات، مع الحفاظ على سلامة واستمرارية الخدمات.

المرجع: الضابط الأمني رقم 2-11 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- أنظمة المعلومات، التطبيقات الويب، الجوال API، قواعد البيانات، الشبكات، والخوادم التابعة لشركة جادتك أو المستضافة لصالحها.
- خدمات البنية التحتية السحابية والموارد التي تؤثر على سرية وسلامة وتوفر بيانات شركة جادتك.
- مختبرات الاختبار الداخلية والمختبرات والموردين الخارجيين الذين يتم تكليفهم بإجراء اختبارات الاختراق.
- الموظفين والموردين والأطراف الثالثة المرتبطين بعمليات اختبار الاختراق.

بنود السياسة

1-21 التخطيط والموافقة

1-1-21 لا يجوز بدء أي اختبار اختراق دون موافقة كتابية مسبقة من الإدارة العليا ومالك الأصل.

2-1-12 يجب إعداد خطة اختبار تتضمن النطاق، الأهداف، طرق الاختبار، الجداول الزمنية، ومعايير التوقف(Rules of Engagement) .

3-1-21 يجب تعريف نقاط الاتصال ومسؤوليات الطوارئ خلال فترة الاختبار.

2-21 التصنيف والنطاق

1-2-21 يتم تحديد الأصول المراد اختبارها وتوثيقها بوضوح.

2-2-21 يمنع توسيع النطاق خارج الحدود المصرح بها دون الحصول على موافقات إضافية.

3-21 المنهجية والمعايير

1-3-21 يجب أن تُجرى الاختبارات وفق منهجيات معتمدة (مثل OSSTMM, OWASP, PTES أو غيرها من أفضل الممارسات)

2-3-21 يجب اختيار الأدوات المناسبة التي تتوافق مع المنهجيات المعتمدة التي تم اختيارها.

3-3-21 يجب توثيق الأدوات والأساليب المستخدمة وتقييم النتائج وفق مقاييس واضحة لخطورة الثغرات.

4-21 السلامة واستمرارية الأعمال

1-4-21 يجب تصميم الاختبارات بحيث تقلل أثرها على الأنظمة الإنتاجية؛ ويفضل إجراء اختبارات في بيئة اختبار أو بنطاقات خارج ساعات الذروة.

2-4-21 يجب تحديد إجراءات إيقاف فوري (Kill Switch) في حال تأثير الاختبار سلبًا على الخدمات أو البيانات.

5-21 السرية وحماية البيانات

1-5-21 يلتزم القائمون بالاختبار بالمحافظة على سرية البيانات التي يتم الوصول إليها أثناء الاختبار وعدم استخدامها أو نشرها خارج نطاق التقرير.

2-5-21 لا يجوز استخراج أو نقل بيانات حساسة دون موافقة مسبقة ومبررة.

21-6 تقرير النتائج والمعالجة

21-6-1 يجب تقديم تقرير مفصل بعد الانتهاء يتضمن نقاط الضعف المكتشفة، مستوى الخطورة، دليل الاستغلال، والتوصيات الإصلاحية.

21-6-2 يجب وضع خطة معالجة واضحة للثغرات المكتشفة مع جداول زمنية للأولوية، ومتابعة التحقق من الإغلاق.(Remediation Verification)

21-7 استخدام مزودي خدمات خارجيين

21-7-1 عند التعاقد مع مزود خارجي لإجراء الاختبارات، يجب التأكد من مؤهلاته، التحقق من سجلّه، توقيع اتفاقية عدم إفشاء(NDA) ، والالتزام بشروط التعاقد والسياسة.

21-8 التوثيق والمراجعة

21-8-1 يجب توثيق جميع أنشطة الاختبار والتقارير والحوادث المرتبطة بها والاحتفاظ بها لفترات زمنية تحددها ضوابط الحفظ.

21-8-2 تراجع سياسة اختبار الاختراق بشكل دوري وتُحدّث وفق تطورات التهديدات والمعايير الفنية.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد خطة الاختبار والموافقة على النطاق وتوفير الموارد والدعم الإداري.
مسؤول الأمن السيبراني	الموافقة على اختبارات الاختراق، التنسيق مع ملاك الأصول، الإشراف على الامتثال، وتقييم المخاطر الناتجة.
فريق اختبار الاختراق / قسم تقنية المعلومات	إعداد خطة الاختبار، إجراء الاختبارات (داخليًا أو عبر مزود خارجي)، توثيق النتائج، وإرشاد فرق المعالجة.
مالكو الأنظمة / فرق التشغيل	تنفيذ إجراءات الإصلاح والتصحيح وفق أولويات التقرير، وإجراء تحقق ما بعد المعالجة.

الجهة / الشخص	المسؤوليات
جميع الموظفين والأطراف ذات الصلة	التعاون مع فرق الأمن وتطبيق إجراءات التخفيف الموقتة عند الحاجة، والامتثال لتوجيهات الاختبار.
مزودو خدمات خارجيون (إن وُجدوا)	تنفيذ اختبارات الاختراق التي يتم التعاقد عليها من قبل طرف خارجي وفق شروط العقد وسياسة شركة جادتك، والالتزام بالسرية والمهنية.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمتعاقدين والموردين المرتبطين بعمليات اختبار الاختراق.
- أي إجراء اختباري غير مصرح به أو خرق للشروط قد يؤدي إلى إجراء اداري أو إجراءات قانونية عند الضرورة.
- تتم مراجعة وتحديث هذه السياسة بشكل دوري لضمان ملاءمتها لأنماط التهديد الجديدة والمعايير الفنية والتنظيمية.

22- سياسة ادارة سجلات الاحداث ومراقبة الامن السيبراني

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات لجمع وتخزين وتحليل سجلات الأحداث في أنظمة شركة جادتك ومراقبة الأنشطة الأمنية للكشف عن الحوادث والتهديدات في الوقت المناسب، وضمان قدرة شركة جادتك على الاستجابة الفعالة للحوادث والحفاظ على سرية وسلامة المعلومات واستمرارية الأعمال.

المرجع: الضابط الأمني رقم 2-12 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- أنظمة التشغيل، التطبيقات، قواعد البيانات، الخوادم، الشبكات، والمكونات التقنية لشركة جادتك.
- سجلات الأحداث المتعلقة بالوصول، التغييرات، النشاطات المشبوهة، والتعامل مع البيانات الحساسة.
- الموظفين والمتعاقدين والأطراف الثالثة الذين لديهم حق الوصول إلى الأنظمة أو مسؤولية إدارة السجلات والمراقبة الأمنية.

بنود السياسة

22-1 جمع السجلات

22-1-1 يجب تسجيل جميع الأحداث المهمة بما في ذلك عمليات الدخول، التغييرات على الأنظمة، أخطاء التطبيقات، والتنبيهات الأمنية.

22-1-2 يتم استخدام أدوات معتمدة لتجميع السجلات من جميع الأنظمة والشبكات والتطبيقات الحيوية.

22-2 حفظ السجلات

22-2-1 يجب تخزين السجلات في مواقع آمنة ومحمية من العبث أو الفقدان.

22-2-2 يتم الاحتفاظ بالسجلات لفترات زمنية محددة وفق متطلبات الامتثال التنظيمي والسياسات الداخلية.

22-3 تحليل ومراقبة السجلات

22-3-1 يتم تحليل السجلات بشكل دوري أو في الوقت الفعلي للكشف عن الأنشطة المشبوهة أو الانتهاكات الأمنية.

22-3-2 يجب إعداد تنبيهات فورية عند اكتشاف أحداث حرجة تهدد سرية وسلامة البيانات أو استمرارية الخدمات.

22-4 الاستجابة للحوادث

22-4-1 عند اكتشاف أي نشاط غير اعتيادي أو حادث أمني، يتم الإبلاغ فوراً لفريق الأمن السيبراني.

22-4-2 يجب توثيق الحادث وتحليل السبب الجذري واتخاذ إجراءات تصحيحية لمنع تكراره.

22-5 الحفاظ على السرية

22-5-1 يجب الحفاظ على سرية سجلات الأحداث وعدم مشاركتها مع أي جهة غير مخولة.

22-5-2 تمنع أي محاولات لتعديل أو حذف السجلات بشكل غير مصرح به.

6-22 التدريب والتوعية

1-6-22 يجب تنفيذ برامج توعية للعاملين حول أهمية سجلات الأحداث وأفضل الممارسات في التعامل مع أنظمة المراقبة الأمنية.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على جمع السجلات، مراقبة الأنشطة، تحليل الحوادث، وضمان الامتثال للسياسات.
قسم تقنية المعلومات / فريق الأمن السيبراني	إعداد أنظمة السجلات، حفظها، مراقبتها، تحليل التنبيهات، وتنفيذ إجراءات الاستجابة للحوادث.
جميع الموظفين	الالتزام بالإجراءات الأمنية عند الوصول للأنظمة، عدم التلاعب بالسجلات، والإبلاغ عن أي نشاط مشبوه.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع المستخدمين والأطراف المرتبطة بالأنظمة التقنية لشركة جادتك.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات إدارية أو قانونية وفق لوائح شركة جادتك.
- تتم مراجعة السياسة بشكل دوري لتحديثها بما يتوافق مع أحدث المعايير الأمنية والتهديدات السيبرانية.

23سياسة ادارة حوادث وتهديدات الامن السيبراني

الغرض

تهدف هذه السياسة إلى وضع إطار شامل لإدارة الحوادث والتهديدات الأمنية، بما يشمل الكشف المبكر، التقييم، الاستجابة، التخفيف من الأضرار، والتعافي، لضمان حماية أصول شركة جادتك الرقمية والبيانات الحساسة واستمرارية الأعمال.

المرجع: الضابط الأمني رقم 2-13 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- الأنظمة، الشبكات، التطبيقات، قواعد البيانات، وأجهزة المستخدمين التابعة لشركة جادتك.
- الحوادث والتهديدات الأمنية التي قد تؤثر على سرية، سلامة أو توفر البيانات والخدمات.
- الموظفين، المتعاقدين، ومقدمي الخدمات الذين لديهم حق الوصول إلى الأنظمة أو دور في إدارة الحوادث الأمنية.

بنود السياسة

1-23 التعريف والتصنيف

1-1-23 تعريف الحوادث والتهديدات الأمنية بشكل واضح (مثل الاختراقات، البرمجيات الضارة، محاولات التصيد، حوادث تسريب البيانات).

2-1-23 تصنيف الحوادث حسب شدتها وتأثيرها (كارثية، حرجة، مرتفعة، متوسطة، منخفضة) لتحديد الأولويات في الاستجابة.

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الكارثة
حادثة كارثية	أعطال كارثية للخدمات أو تأثير سلبي على الأمن السيبراني الوطني بحيث تؤدي إلى أو تهدد بإحداث مضاعفات اقتصادية أو اجتماعية خطيرة، أو تؤدي لفقدان حياة بعض الأشخاص.	فورا	فورا
حادثة حرجة	ضرر جسيم يؤثر بشكل مباشر على سمعة شركة جادتك، أو يؤثر على جادتك ومصداقيتها، أو يؤثر على العديد من وحدات الأعمال الوظيفية فيها، مما يستدعي تنفيذ إجراءات استمرارية الأعمال.	فورا	ساعتان
حادثة مرتفعة	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع الإلكتروني.	ساعة او ساعتان	5-4 ساعات
حادثة متوسطة	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في شركة جادتك.	3-2 ساعات	9-8 ساعات
حادثة منخفضة	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	5 ساعات	يوم

2-23 الكشف والمراقبة

1-2-23 استخدام أنظمة مراقبة للكشف المبكر عن الحوادث والتهديدات.

2-2-23 تسجيل وتحليل جميع التنبيهات والأنشطة المشبوهة لضمان استجابة سريعة.

3-23 الاستجابة والتخفيف

1-3-23 اتخاذ إجراءات فورية لعزل الأجهزة أو الأنظمة المتأثرة وتقليل الأضرار المحتملة.

2-3-23 تنفيذ خطط الاستجابة للحوادث وفق مستوى التصنيف وتنسيق الفرق المعنية.

4-23 التوثيق والتقرير

1-4-23 توثيق كل حادث أو تهديد، بما في ذلك السبب الجذري، الإجراءات المتخذة، والنتائج النهائية.

2-4-23 إعداد تقارير دورية لإدارة شركة جادتك لتقييم الوضع الأمني وفعالية الإجراءات المتخذة.

5-23 التعافي واستمرارية الأعمال

1-5-23 استعادة الأنظمة والبيانات المتأثرة بشكل آمن بعد معالجة الحادث.

2-5-23 تقييم الإجراءات التصحيحية لتجنب الوقوع في هذا الحدث مرة أخرى ومنع تكرار الحوادث المشابهة.

6-23 التدريب والتوعية

1-6-23 تقديم برامج تدريب وتوعية لجميع الموظفين حول كيفية التعرف على الحوادث الأمنية السيبرانية والتصرف المناسب عند حدوثها.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها.
مسؤول الأمن السيبراني	الإشراف على إدارة الحوادث، مراجعة التصنيف، متابعة الاستجابة، وضمان الامتثال للسياسات.
قسم تقنية المعلومات / فريق الأمن السيبراني	مراقبة الأنظمة، الكشف عن الحوادث، توثيقها، تنسيق الاستجابة، وتنفيذ الإجراءات التصحيحية.
جميع الموظفين	الالتزام بالإجراءات الأمنية، الإبلاغ الفوري عن أي حادث أو نشاط مشبوه، والتعاون مع فرق الاستجابة.
مزودو خدمات خارجيون (إن وُجدوا)	التعامل مع مزودي الخدمات الخارجيين عند الحاجة لدعم الاستجابة للحوادث وفق السياسة والعقد المبرم.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمتعاقدين والأطراف المرتبطة بأنظمة شركة جادتك.
- أي مخالفة للسياسة أو الإهمال في الإبلاغ عن الحوادث قد يؤدي إلى إجراءات ادارية أو قانونية.
- تتم مراجعة هذه السياسة بشكل دوري لتحديثها بما يتوافق مع أحدث التهديدات والتقنيات والمعايير التنظيمية.

24- سياسة الامن السيبراني المتعلقة بالأمن المادي-

الغرض

تهدف هذه السياسة إلى حماية البنية التحتية التقنية لشركة جادتك، ومراكز البيانات، والمكاتب، والمرافق التي تحتوي على أصول رقمية من الوصول غير المصرح به أو التلف أو السرقة، وضمان دمج ضوابط الأمن المادي ضمن إطار الأمن السيبراني للحفاظ على سرية وسلامة وتوفر المعلومات.

المرجع: الضابط الأمني رقم 2-14 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- مراكز البيانات، غرف الخوادم، المكاتب، والمرافق التي تحتوي على أصول رقمية أو بيانات حساسة.
- الموظفين، المتعاقدين، الزوار، والموردين الذين لديهم وصول مادي إلى المرافق أو الأجهزة التقنية.
- الأجهزة، الخوادم، الشبكات، وسائط التخزين، والأنظمة المستخدمة في بيئة العمل.

بنود السياسة

1-24 الوصول المادي والتحكم

1-1-24 السماح بالوصول للمرافق الحساسة فقط للأشخاص المصرح لهم.

2-1-24 استخدام وسائل تحكم بالوصول مثل البطاقات الذكية، الأقفال الإلكترونية، أو البصمة.

3-1-24 تسجيل دخول وخروج جميع الأفراد من المرافق الحساسة وتخزين السجلات لمراجعتها عند الحاجة.

2-24 المراقبة والفحص

1-2-24 تركيب أنظمة مراقبة بالفيديو وأجهزة إنذار في المواقع الحيوية.

2-2-24 مراقبة الأنشطة المشبوهة أو غير الاعتيادية داخل المرافق الحساسة.

3-2-24 إجراء فحوصات دورية للتأكد من فعالية أجهزة المراقبة والإنذار.

3-24حماية الأجهزة والبيانات

1-3-24 وضع الأجهزة والخوادم في مواقع آمنة داخل المرافق لمنع الوصول غير المصرح به.

2-3-24 حماية وسائط التخزين والأصول التقنية باستخدام خزائن أو غرف آمنة.

3-3-24 التأكد من التخلص الآمن من الأجهزة والوسائط عند انتهاء استخدامها.

4-24 الإجراءات عند الحوادث

1-4-24 الإبلاغ فوراً عن أي اختراق مادي أو فقدان أو سرقة أصول تقنية.

2-4-24 عزل المرافق المتأثرة والتحقق من سلامة الأنظمة والبيانات.

3-4-24 توثيق الحادث وتحليل السبب الجذري واتخاذ الإجراءات التصحيحية لمنع تكراره.

5-24 التوعية والتدريب

1-5-24 تدريب الموظفين والمتعاقدين على إجراءات الأمن المادي وأهمية حماية الأصول التقنية.

2-5-24 توعية الموظفين حول التهديدات المرتبطة بالوصول المادي غير المصرح به وكيفية التصرف عند وقوع حادث.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	مراقبة تنفيذ ضوابط الأمن المادي، مراجعة سجلات الوصول، وضمان الامتثال للسياسات.
قسم تقنية المعلومات / فرق الأمن المادي	إدارة أنظمة التحكم بالوصول والمراقبة، فحص الأجهزة، وتنسيق الاستجابة للحوادث المادية.
جميع الموظفين والمتعاقدين	الالتزام بالإجراءات الأمنية، استخدام وسائل الدخول المصرح بها، والإبلاغ عن أي نشاط مريب.
الموردون الخارجيون (إن وُجدوا)	متابعة وإدارة الإجراءات المادية مع الموردين الخارجيين عند الحاجة.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمتعاقدين والأطراف المرتبطة بالمرافق أو الأنظمة التقنية لشركة جادتك.
- أي خرق للسياسة قد يؤدي إلى إجراءات ادارية أو قانونية وفق اللوائح الداخلية لشركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لتحديثها بما يتوافق مع أحدث التهديدات المادية والمعايير الأمنية.

25- سياسة حماية تطبيقات الويب

الغرض

تهدف هذه السياسة إلى حماية تطبيقات الويب التابعة لشركة جادتك من الهجمات السيبرانية والاختراقات، بما في ذلك تهديدات مثل الحقن البرمجي، الهجمات عبر المصادقة، هجمات البرمجيات الضارة، وتسريب البيانات، لضمان سرية وسلامة وتوافر المعلومات والخدمات المقدمة عبر الإنترنت.

المرجع: الضابط الأمني رقم 2-15 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- تطبيقات الويب التي تطورها شركة جادتك أو تستخدمها سواء كانت داخلية أو خارجية.
- الخوادم، قواعد البيانات، واجهات برمجة التطبيقات(APIs) ، وخدمات الويب المرتبطة بالتطبيقات.
- الموظفين، المتعاقدين، والموردين الذين يشاركون في تطوير، صيانة، أو إدارة تطبيقات الويب.

بنود السياسة

1-25 تطوير التطبيقات الآمن

1-1-25 اتباع أفضل ممارسات تطوير التطبيقات الآمنة وفق معايير OWASP Top 10.

25-1-2 إجراء مراجعات الأمان (Security Reviews) أثناء مراحل التصميم والتطوير.

25-1-3 منع إدخال الأكواد الضارة أو غير الموثوقة في بيئة التطوير والإنتاج.

25-1-4 يجب على تطبيقات الويب الخارجية اتباع مبدأ البنية متعددة الطبقات Multi-Tier Architecture بحيث لا تقل عن طبقتين Two-Tier Architecture لتعزيز الامان وفصل المهام داخل النظام.

25-1-5 بالنسبة للأنظمة الحساسة، يجب استخدام بنية متعددة الطبقات Multi-Tier Architecture لا تقل عن ثلاث طبقات Three-Tier Architecture لضمان حماية اعلى وفصل افضل للوظائف الحساسة.

25-1-6 يجب الفصل بين بيئة التطوير Development Environment وبيئة الاختبار Testing Environment وبيئة الانتاج Production Environment ، بحيث يتم تنفيذ التطوير والاختبارات في بيئات منفصلة قبل النشر في بيئة العمل الفعلية.

25-2 اختبار الأمان

25-2-1 إجراء اختبارات أمنية دورية لتطبيقات الويب تشمل اختبارات الاختراق والفحص الأمني (Vulnerability Scanning & Penetration Testing).

25-2-2 معالجة الثغرات المكتشفة حسب مستوى الخطورة وفي إطار زمني محدد.

25-3 المصادقة وإدارة الجلسات

25-3-1 تطبيق سياسات موثوقة لكلمات المرور والمصادقة متعددة العوامل (MFA) حيثما أمكن.

25-3-2 حماية الجلسات (Sessions) باستخدام آليات آمنة لمنع الاختراق أو الانتحال.

25-4 حماية البيانات

25-4-1 يجب استخدام بروتوكولات الاتصال الآمن Secure Communication Protocols مثل HTTPS و SFTP و TLS عند نقل البيانات او الوصول للأنظمة.

25-4-2 منع التسريب العرضي للبيانات عبر التحكم في الوصول وإعدادات الأذونات.

25-5 مراقبة الأنشطة والتسجيل

25-5-1 تسجيل وتحليل نشاطات المستخدمين والأنظمة للكشف عن محاولات الاختراق أو الأنشطة غير الطبيعية.

25-5-2 الاحتفاظ بسجلات الأمان وفق فترة الاحتفاظ المعتمدة من قبل شركة جادتك.

25-6 الاستجابة للحوادث

25-6-1 الإبلاغ الفوري عن أي حادث أمني يتعلق بتطبيقات الويب إلى فريق الأمن السيبراني.

25-6-2 توثيق الحوادث، تقييم الأثر، واتخاذ الإجراءات التصحيحية لتجنب تكرارها.

25-7 التوعية والتدريب

25-7-1 تدريب المطورين وفرق الصيانة على أساليب البرمجة الآمنة وأحدث تهديدات تطبيقات الويب.

25-7-2 توعية الموظفين حول استخدام التطبيقات بشكل آمن وتقنيات الحماية الأساسية.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على تنفيذ السياسات الأمنية، مراجعة نتائج الاختبارات، وضمان الامتثال للمعايير.
فرق تطوير التطبيقات / قسم تقنية المعلومات	تطوير التطبيقات وفق معايير الأمان، إدارة أنظمة الاختبارات، معالجة الثغرات، ومراقبة الأنشطة.
جميع الموظفين والمستخدمين المصرح لهم	الالتزام بإرشادات الاستخدام الآمن للتطبيقات، والإبلاغ عن أي سلوك مشبوه أو ثغرات مكتشفة.
مزودو خدمات خارجيون (إن وُجدوا)	تنفيذ اختبارات الأمان عند التعاقد مع مزودي خدمات خارجية وفق شروط العقد وسياسة شركة جادتك.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمطورين والمتعاقدين والأطراف المرتبطة بتطبيقات الويب.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات إدارية أو قانونية وفق لوائح شركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لتحديثها بما يتوافق مع أحدث التهديدات والمعايير الأمنية الخاصة بتطبيقات الويب.

26- سياسة الامن السيبراني ضمن استمرارية الاعمال

الغرض

تهدف هذه السياسة إلى دمج ضوابط الأمن السيبراني ضمن خطط استمرارية الأعمال لشركة جادتك، لضمان حماية البيانات والأنظمة الحيوية واستعادة العمليات بشكل سريع وفعال عند وقوع أي حادث سيبراني أو كارثة تؤثر على بيئة العمل.

المرجع: الضابط الأمني رقم 3-1 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- الأنظمة، الشبكات، التطبيقات، قواعد البيانات، والأجهزة التقنية الأخرى المستخدمة في العمليات الحيوية لشركة جادتك.
- خطط واستراتيجيات استمرارية الأعمال والتعافي من الكوارث.(BC/DR)
- الموظفين والمتعاقدين والأطراف الخارجية المرتبطة بتطبيق خطط استمرارية الأعمال أو التعامل مع الأنظمة الحيوية.

بنود السياسة

1-26 تحديد الأنظمة والبيانات الحيوية

1-1-26 تحديد وتصنيف الأنظمة والبيانات الحيوية وفق تأثيرها على العمليات الأساسية لشركة جادتك.

2-1-26 وضع ضوابط أمنية خاصة لحماية هذه الأنظمة والبيانات أثناء الحوادث.

2-26 تكامل الأمن السيبراني مع خطط الاستمرارية

1-2-26 تضمين ضوابط الأمن السيبراني ضمن خطط استمرارية الأعمال والتعافي من الكوارث.

2-2-26 التأكد من أن خطط الاستمرارية تشمل سيناريوهات الحوادث السيبرانية مثل الاختراقات، البرمجيات الضارة، أو تسرب البيانات.

3-26 النسخ الاحتياطي والاستعادة

1-3-26 تنفيذ عمليات النسخ الاحتياطي للبيانات والأنظمة الحيوية وفق جدول زمني محدد.

2-3-26 اختبار استعادة البيانات والأنظمة بشكل دوري للتأكد من فعاليتها في حالات الطوارئ.

4-26 التحكم في الوصول وإدارة الهوية

1-4-26 تفعيل إجراءات موثوقة للتحكم بالوصول إلى الأنظمة الحيوية أثناء الحوادث.

2-4-26 ضمان استخدام المصادقة متعددة العوامل (MFA) لحماية الأنظمة الحساسة.

5-26 مراقبة الأنشطة والاستجابة للحوادث

1-5-26 مراقبة الأنشطة على الأنظمة الحيوية للكشف المبكر عن الحوادث السيبرانية.

2-5-26 تنفيذ خطط استجابة للحوادث لضمان استمرارية الأعمال وتقليل الأضرار.

6-26 التدريب والتوعية

1-6-26 تدريب موظفين الامن السيبراني على دورهم في استمرارية الأعمال وحماية الأنظمة أثناء الحوادث.

2-6-26 رفع مستوى الوعي لدى موظفين شركة جادتك عن التهديدات السيبرانية وتأثيرها على استمرارية العمل.

7-26 مراجعة وتحسين الخطط

1-7-26 مراجعة دورية لخطط استمرارية الأعمال لضمان توافقها مع أحدث تهديدات الأمن السيبراني.

2-7-26 تحديث السياسات والإجراءات بناءً على نتائج الاختبارات والدروس المستفادة من الحوادث السابقة.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها.
مسؤول الأمن السيبراني	الإشراف على دمج الأمن السيبراني ضمن خطط استمرارية الأعمال، متابعة الاختبارات، وضمان الامتثال للمعايير.
قسم تقنية المعلومات / فرق الأمن السيبراني	تنفيذ ضوابط النسخ الاحتياطي والاستعادة، مراقبة الأنظمة الحيوية، والاستجابة للحوادث.
جميع الموظفين والمتعاقدين	الالتزام بالإجراءات المحددة في خطط استمرارية الأعمال، الإبلاغ عن الحوادث، والمشاركة في التدريبات والتمارين.
الموردون الخارجيون (إن وُجدوا)	دعم العمليات أثناء الحوادث والتعاون مع فرق الاستجابة لضمان استعادة العمليات.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمتعاقدين والأطراف المرتبطة بالأنظمة الحيوية وخطط استمرارية الأعمال.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات ادارية أو قانونية وفق اللوائح الداخلية لشركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع أحدث التهديدات والتقنيات ومتطلبات استمرارية الأعمال.

27- سياسة الامن السيبراني المتعلقة بالأطراف الخارجية

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات للأمن السيبراني عند التعامل مع الأطراف الخارجية، بما في ذلك الموردين، المتعاقدين، ومزودي الخدمات، لضمان حماية بيانات شركة جادتك وأنظمتها من المخاطر الناشئة عن الوصول الخارجي أو التعامل مع أطراف خارجية.

المرجع: الضابط الأمني رقم 4-1 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- الموردين، المتعاقدين، والشركاء الخارجيين الذين لديهم حق الوصول إلى أنظمة شركة جادتك أو بياناتها.
- التعاقدات والعقود الجديدة أو القائمة التي تتضمن الوصول إلى بيانات أو أنظمة شركة جادتك.
- الموظفين المسؤولين عن إدارة العلاقة مع الأطراف الخارجية والمخولين لإعطاء الوصول إلى الموارد التقنية.

بنود السياسة

1-27 تقييم المخاطر للأطراف الخارجية

1-1-27 إجراء تقييم شامل للمخاطر السيبرانية قبل منح أي طرف خارجي الوصول إلى الأنظمة أو البيانات.

2-1-27 تحديد مستوى الوصول المطلوب وفق مبدأ أقل قدر من الصلاحيات .(Least Privilege)

2-27 العقود والاتفاقيات

1-2-27 تضمين شروط أمنية سيبرانية واضحة في العقود مع الأطراف الخارجية تشمل التزامات الخصوصية، حماية البيانات، وإجراءات الاستجابة للحوادث.

2-2-27 توقيع اتفاقيات عدم إفشاء (NDA) بين الأطراف لضمان سرية المعلومات.

3-27 التحكم في الوصول وإدارة الهوية

1-3-27 منح الأطراف الخارجية الوصول للأنظمة والبيانات المصرح بها.

2-3-27 استخدام وسائل مصادقة موثوقة، وتفعيل المصادقة متعددة العوامل (MFA) عند الحاجة.

3-3-27 مراجعة الوصول بشكل دوري وإلغاءه فور انتهاء الحاجة أو انتهاء العقد.

4-27 مراقبة الأنشطة والتدقيق

1-4-27 مراقبة الأنشطة التي يقوم بها الأطراف الخارجية ضمن أنظمة شركة جادتك.

2-4-27 إجراء تدقيق دوري للتأكد من التزام الأطراف الخارجية بسياسات الأمان.

5-27 الاستجابة للحوادث

1-5-27 إلزام الأطراف الخارجية بالإبلاغ الفوري عن أي حادث أو تهديد قد يؤثر على بيانات أو أنظمة شركة جادتك.

2-5-27 تنسيق إجراءات الاستجابة بين شركة جادتك والطرف الخارجي عند وقوع أي حادث.

3-5-27 لا بد من موافقة شركة جادتك في حال الحاجة الى تدخل طرف ثالث.

6-27 التوعية والتدريب

1-6-27 التأكد من أن الأطراف الخارجية على دراية بسياسات الأمان الأساسية ومتطلبات حماية البيانات.

2-6-27 تقديم التوجيه اللازم لموظفي شركة جادتك المتعاملين مع الأطراف الخارجية حول أفضل ممارسات الأمان.

8-27 مراجعة وتحسين السياسة

27-8-1 مراجعة دورية لعقود الأطراف الخارجية وسياسات الأمان لضمان توافقها مع أحدث التهديدات والمعايير التنظيمية.

27-8-2 تحديث السياسات والإجراءات وفق الدروس المستفادة من الحوادث أو نتائج التدقيق.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على تقييم المخاطر، مراجعة العقود، متابعة الامتثال، وضمان دمج الضوابط الأمنية في التعاقدات.
قسم تقنية المعلومات / فرق الأمن السيبراني	تنفيذ الضوابط التقنية، إدارة الوصول، مراقبة الأنشطة، وتنسيق الاستجابة للحوادث مع الأطراف الخارجية.
جميع الموظفين	الالتزام بسياسات شركة جادتك، استخدام الأنظمة وفق التعليمات، والإبلاغ عن أي حادث أو نشاط مشبوه.
الأطراف الخارجية / الموردون / المتعاقدون	الالتزام بالشروط الأمنية المتفق عليها في العقد وإبلاغ شركة جادتك فوراً عن أي حادث يؤثر على البيانات أو الأنظمة.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والأطراف الخارجية المتعاقد معها.
- أي مخالفة قد تؤدي إلى إجراءات ادارية أو قانونية وفق لوائح شركة جادتك، وقد تشمل إنهاء العقود عند الضرورة.
- تتم مراجعة السياسة بشكل دوري لتحديثها وفق أحدث المتطلبات الأمنية والتهديدات السيبرانية.

28- سياسة الامن السيبراني المتعلقة بالحوسبة السحابية والاستضافة

الغرض

تهدف هذه السياسة إلى وضع ضوابط وإجراءات لحماية البيانات والأنظمة المستضافة على بيئات الحوسبة السحابية أو ضمن خدمات الاستضافة الخارجية، لضمان سرية وسلامة وتوافر المعلومات والأنظمة، وتقليل المخاطر السيبرانية المرتبطة بالخدمات السحابية في شركة جادتك.

المرجع: الضابط الأمني رقم 4-2 من لوائح الهيئة الوطنية للأمن السيبراني.

نطاق العمل

تنطبق هذه السياسة على:

- الخدمات والأنظمة والتطبيقات المستضافة على منصات الحوسبة السحابية (Cloud)لشركة جادتك او لدى مزودي خدمات الاستضافة الخارجيين.
- البيانات المخزنة أو المعالجة أو المنتقلة عبر هذه البيئات.
- الموظفين والمتعاقدين والموردين الذين لهم حق الوصول إلى الأنظمة أو البيانات في هذه البيئات.

بنود السياسة

1-28 اختيار مزودي الخدمات السحابية والاستضافة

1-1-28 استخدام مزودين موثوقين يلتزمون بمعايير الأمان الدولية والمحلية.

2-1-28 التأكد من وجود اتفاقيات مستوى الخدمة (SLA) واضحة تشمل الضمانات الأمنية وحماية البيانات.

2-28 التحكم في الوصول وإدارة الهوية

1-2-28 منح الوصول فقط للأشخاص المصرح لهم وفق مبدأ أقل قدر من الصلاحيات (Least Privilege).

2-2-28 تفعيل المصادقة متعددة العوامل (MFA) لجميع المستخدمين الذين لديهم صلاحيات حساسة.

3-2-28 مراجعة الأذونات بشكل دوري وإلغاء الوصول عند انتهاء الحاجة أو انتهاء العقد.

3-28 حماية البيانات

1-3-28 تشفير البيانات أثناء النقل (TLS/HTTPS) وعند التخزين إذا كانت حساسة.

2-3-28 تطبيق سياسات النسخ الاحتياطي المنتظمة وضمان إمكانية الاستعادة عند الحاجة.

4-28 مراقبة الأنشطة والتدقيق

1-4-28 مراقبة الأنشطة على الأنظمة السحابية بشكل دوري أو في الوقت الفعلي للكشف عن التهديدات أو الأنشطة غير الطبيعية.

2-4-28 الاحتفاظ بسجلات النشاط وفق فترة الحفظ المعتمدة ومراجعتها عند الحاجة.

5-28 التعامل مع الثغرات والحوادث

1-5-28 إشراك مزودي الخدمات في الكشف المبكر عن الثغرات والاستجابة للحوادث الأمنية.

2-5-28 توثيق أي حادث، تقييم الأثر، واتخاذ الإجراءات التصحيحية بالتنسيق مع فريق الأمن السيبراني.

6-28 التوافق والامتثال

1-6-28 التأكد من التزام مزودي الخدمات بالقوانين المحلية والدولية المتعلقة بحماية البيانات والخصوصية.

2-6-28 مراجعة دورية للعقود والسياسات لضمان الامتثال للمعايير التنظيمية والأمنية.

7-28 التوعية والتدريب

1-7-28 تدريب الموظفين على الاستخدام الآمن للأنظمة السحابية والاستضافة، واستيعاب التهديدات المتعلقة بالحوسبة السحابية.

2-7-28 توعية الفرق التقنية حول أفضل ممارسات إدارة الأمان في بيئات الحوسبة السحابية.

الأدوار والمسؤوليات

الجهة / الشخص	المسؤوليات
الإدارة العليا	اعتماد السياسة وتوفير الموارد اللازمة لتطبيقها.
مسؤول الأمن السيبراني	الإشراف على تنفيذ الضوابط الأمنية في البيئات السحابية والاستضافة، مراجعة الامتثال، ومتابعة الحوادث.
قسم تقنية المعلومات / فرق الأمن السيبراني	إدارة الوصول، مراقبة الأنشطة، إدارة النسخ الاحتياطية، والاستجابة للحوادث على الأنظمة السحابية.
جميع الموظفين والمتعاقدين	الالتزام بسياسات الاستخدام الآمن للحوسبة السحابية، والإبلاغ عن أي تهديد أو نشاط مشبوه.
مزودو الخدمات الخارجية	ضمان الامتثال للعقود والاتفاقيات الأمنية عند تقديم خدمات الاستضافة أو الحوسبة السحابية.

الالتزام بالسياسة

- الالتزام بهذه السياسة إلزامي لجميع الموظفين والمتعاقدين والأطراف الخارجية المرتبطة بالأنظمة السحابية أو خدمات الاستضافة.
- أي مخالفة للسياسة قد تؤدي إلى إجراءات ادارية أو قانونية وفق اللوائح الداخلية لشركة جادتك.
- تتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع أحدث التهديدات، التقنيات، والمعايير الأمنية للحوسبة السحابية.