مؤسسة كيو سن للسلام والتنمية الإعلامية
Q Sun Foundation for Peace and Media Development

سياسات الحوكمة

سياسة أمن المعلومات العامة

سياسات مؤسسة كيو سن للسلام والتنمية الإعلامية

الجهة
مؤسسة كيو سن

رمز الوثيقة
حـ ١١

التعريف والأهداف والنطاق

١. تعريف سياسة أمن المعلومات

هي مجموعة القواعد والعمليات والإجراءات التي تُطبّق عند التعامل مع المعلومات والتقنيات المرتبطة بها داخل المؤسسة، وتمنع التهديدات التي تستهدف البيانات والمعلومات، للمحافظة على مستويات مقبولة من حماية السرية وضمان التكامل وتوفير إتاحة المعلومات.

٢. أهداف السياسة

2.1. تأكيد التزام قيادة المؤسسة ونيتها في دعم أهداف ومبادئ حماية المعلومات بما يتوافق مع إجراءات العمل.

2.2. إعداد منهجية لأمن المعلومات في المكتب التنفيذي والفروع التابعة له.

2.3. تعريف المستخدمين بالتزاماتهم وواجباتهم المطلوبة تجاه أمن نظم المعلومات.

2.4. بيان الإجراءات الواجب اتباعها لتفادي المخاطر والتهديدات والتعامل معها إذا وقعت.

2.5. تحديد آليات تنفيذ المسؤوليات والواجبات لكل مستخدم.

٣. مرجعية السياسة

ترتكز السياسة على معيار التوافق الأمني ISO 27001 ومعيار قواعد الممارسة لإدارة أمن المعلومات ISO 27002.

٤. النطاق

تسري السياسة على جميع مستخدمي الأصول المعلوماتية للمؤسسة وجميع مستخدمي شبكتها، بغض النظر عن موقعهم الجغرافي.

الأدوار والمسؤوليات

٥.١ دور قيادة المؤسسة

5.1.1. دعم تنفيذ سياسات الحماية في المؤسسة لحماية الأصول المعلوماتية.

5.1.2. ضمان توافق السياسات مع أهداف المؤسسة واستراتيجيتها وإجراءات عملها.

5.1.3. الموافقة على استخدام جميع نظم المعلومات المستخدمة في معالجة المعلومات وتخزينها وطباعتها.

5.1.4. الموافقة على السياسات الجديدة أو التعديلات على السياسات الحالية.

٥.٢ دور قسم تقنية المعلومات

5.2.1. تحديد إجراءات تنفيذ السياسة والعمل على تنفيذها.

5.2.2. توزيع وثائق حماية المعلومات ونشرها بالبريد أو وسائل التواصل لجميع المستخدمين.

5.2.3. ضمان حماية نظم المعلومات والبنية التحتية وفق الآليات التقنية التي حددها مصممو الأنظمة والبرمجيات.

5.2.4. مراقبة حماية الأنظمة والتطبيقات والشبكة.

5.2.5. تحديد سياسات حماية المعلومات وإدامتها ومراعاة معايير السياسة الأمنية في الأنظمة المطوّرة داخليًا.

5.2.6. إعداد معايير حماية المعلومات اللازمة لرفع مستوى الحماية في المؤسسة وتحديثها دوريًا.

5.2.7. تطبيق ضوابط ملائمة لحماية سرية المعلومات الحساسة وسلامتها وأصالتها.

5.2.8. مراجعة السياسات والإجراءات ومعايير الحماية وتحديثها سنويًا.

5.2.9. ضمان توثيق سياسات الحماية الداخلية والإجراءات والمعايير ذات الصلة بما ينسجم مع المعايير العالمية والمتطلبات القانونية والتنظيمية.

المسؤوليات والالتزام والاستثناءات

٥.٢ دور قسم تقنية المعلومات · تتمة

5.2.10. تحديد إجراءات تنفيذ السياسة والعمل على تنفيذها على مستوى أجهزة الحاسوب والتركيبات الشبكية.

5.2.11. تطبيق ضوابط ملائمة لحماية سلامة الأجهزة وما تحتويه من بيانات.

5.2.12. توفير التدريب المناسب للمتعاملين مع البيانات والمعلومات والمستخدمين لها.

5.2.13. مراجعة استمرار فعالية السياسات الأمنية وملاءمتها ومستوى الأمن في تقنية المعلومات.

5.2.14. اقتراح تحديث المكونات التي لا تحقق المستوى المطلوب من الأمن أو استبدالها عند الحاجة.

5.2.15. إجراء تقييم سنوي لفعالية الضوابط المطبقة مع مراعاة آراء المستخدمين ذوي العلاقة، ونتائج المراجعة المستقلة ومراجعة الإدارة، واتجاهات التهديدات ونقاط ضعف الحماية.

٥.٣ الدوائر والمستخدمون

5.3.1. الالتزام بسياسات وإرشادات ومعايير وإجراءات حماية المعلومات.

5.3.2. الإبلاغ عن نقاط ضعف الحماية الفعلية أو المشتبه في وجودها والتي تؤثر على سرية المعلومات الحساسة وسلامتها وتوافرها.

5.3.3. استخدام المعلومات وفق سياسة الاستخدام المقبول فقط.

5.3.4. تتعاون جميع الإدارات فيما بينها ومع قسم تقنية المعلومات لضمان مستوى حماية ملائم لأصولها المعلوماتية.

٦. الالتزام

التقيد بالسياسات والإرشادات والمعايير والإجراءات إلزامي على جميع المستويات. وتؤدي أي مخالفة أو انتهاك إلى إجراءات وعقوبات تتناسب مع مستواها، وقد تصل إلى إنهاء الخدمة.

٧. الاستثناءات

تعالج السياسة متطلبات حماية المعلومات. وعند الحاجة، يُقدّم طلب استثناء رسمي إلى قسم تقنية المعلومات مع بيان أسبابه. ويشترط موافقة قيادة المؤسسة والضرورة القصوى وتحديد مدة مؤقتة للاستثناء.

السياسات المرتبطة

استنادًا إلى أفضل الممارسات وتوصيات معيار ISO 27001، تُطبق السياسات الرئيسية الآتية لحماية المعلومات داخل المؤسسة.

8.1.1. سياسة كلمة المرور.

8.1.2. سياسة التحكم في الوصول.

8.1.3. سياسة إدارة الأصول.

8.1.4. سياسة إدارة المخاطر.

8.1.5. سياسة النسخ الاحتياطي للبيانات.

8.1.6. سياسة الأمن المادي والبيئي.

8.1.7. سياسة أمن الموارد البشرية.

8.1.8. سياسة حيازة نظم المعلومات وتطويرها وصيانتها.

8.1.9. سياسة التعامل مع حوادث أمن المعلومات.

8.1.10. سياسة إدارة استمرارية العمل.

8.1.11. سياسة التوثيق.

8.2. تعد هذه السياسات عامة، وتتضمن كل منها مجموعة من السياسات الفرعية. وتصدر بحسب الأهمية، وتتضمن كل سياسة التعريف والغرض والنطاق ومحور السياسة.

8.3. لا يعبر ترتيب ورود السياسات عن أهميتها، فجميعها مهمة بحسب الظرف.

8.4. تُصدر كل سياسة ويُعمّم تطبيقها على حدة بعد إقرارها من قيادة المؤسسة.

محور السياسة · المسؤولية والوصول

9.1. أمن المعلومات مسؤولية الجميع، كل بحسب موقعه. ويعي جميع موظفي المؤسسة مسؤوليتهم عن الالتزام بسياسات وإجراءات ومعايير حماية المعلومات، والامتثال لمتطلبات حماية البيانات وسياسة أمن المعلومات.

9.2. الجهل بالسياسات الأمنية عذر غير مقبول.

9.3. تتعاون جميع الإدارات مع قسم تقنية المعلومات لتوفير مستويات مقبولة لحماية أصولها المعلوماتية.

9.4. يقتصر الدخول إلى المعلومات أو تعديلها أو تحديثها على الأفراد المصرح لهم رسميًا.

9.5. يكون الوصول إلى موارد المؤسسة ومعلوماتها ضمن نطاق الصلاحيات الممنوحة.

9.6. تُستخدم موارد المؤسسة ومعلوماتها للأغراض المعتمدة والموافق عليها فقط.

9.7. يتحمل كل من فُوّض بالدخول إلى موارد المؤسسة ومعلوماتها كامل المسؤولية عن استخدامها على نحو مناسب وحمايتها وتجنب الأفعال التي تسبب مخاطر.

9.8. يُمنع الوصول إلى الموارد والمعلومات التي لم يُمنح المستخدم تصريحًا بالوصول إليها.

9.9. لا يجوز استخدام موارد وأنظمة شخصية على أجهزة المؤسسة وشبكتها دون تصريح.

9.10. يُمنع استخدام أي أنظمة أو طرق تؤدي إلى اختراق الشبكة والأنظمة أو الحصول على امتيازات غير مصرح بها.

9.11. تخضع جميع وسائل الوصول عن بعد لمصادقة الوصول إلى الخدمات من الأنظمة المسؤولة.

9.12. يقتصر الوصول والاتصال من الشبكات الواسعة وإليها على المستخدمين المخولين فقط.

9.13. تُحصر الموارد والأنظمة والمعلومات في المؤسسة وفروعها وتُحدد وتُصنّف بحسب طبيعتها لتيسير الرجوع إليها.

محور السياسة · الرقابة والحماية

9.14. تُحدد في جميع الأنظمة المستخدمة نقطة وصول ترتبط بإجراءات المراقبة والتدقيق عبر مميز فريد قابل للتتبع وهوية دخول وكلمة مرور، باستثناء الأنظمة المصممة للوصول المفتوح والعام، مع مراعاة المعايير الأخرى.

9.15. للمؤسسة منع المستخدمين من الوصول إلى مواردها وأنظمتها ومراقبة جميع عمليات استخدامها، بغض النظر عن الأدوات والوسائل المستخدمة، بصفتها مالكة لها.

9.16. تُحدد جميع الحوادث والمخاطر التي تؤثر أو قد تؤثر في أمن المعلومات، وتُوضع خطط وإجراءات مناسبة لمواجهتها.

9.17. تُتخذ التدابير المناسبة لتأمين معدات الشبكة ومصادرها وتمديداتها والطاقة ووسائل الاتصال المختلفة.

9.18. تُتبع تدابير وضوابط خاصة عند نقل الموارد والمعلومات خارج المؤسسة بأي طريقة.

9.19. تُوفر آليات ملائمة للوقاية من المخاطر، مثل وسائل الحماية المادية وبرامج مكافحة الفيروسات وأنظمة تحري الاختراق وأنظمة المراقبة والتحقق الأخرى.

9.20. يجب الإبلاغ عن أي محاولات اختراق أو تهديد لأمن المعلومات.

9.21. تُنظّم برامج ودورات وندوات لرفع مستوى الوعي الأمني وتعزيزه.

9.22. تُراجع السياسات الأمنية وتُحدّث دوريًا.

9.23. تُجرى عمليات فحص مناسبة بانتظام لتحديد حالات الضعف والقصور الأمني.

9.24. تُطبّق سياسة المكتب التنفيذي في جميع مكاتب المؤسسة.

9.25. يجوز عند الحاجة الاستعانة بطرف من خارج المؤسسة للمساعدة في تطبيق أساليب حماية الموارد والأنظمة المعلوماتية أو صيانتها أو حل أي مشكلات أمنية أخرى.