السياسة العامة لأمن المعلومات

وفق المواصفة الدولية ISO/IEC 27001:2022

WI-02

يلتزم مصرف العراق الأول الإسلامي للاستثمار والتمويل بتطبيق وتحسين نظام إدارة أمن المعلومات (ISMS) وفق المواصفة الدولية ISO/IEC 27001:2022 والمتطلبات الرقابية والقانونية والتعاقدية ذات العلاقة، بما يضمن سرية المعلومات وسلامتها وتوافرها.

وتلتزم الإدارة العليا بتوفير القيادة والموارد اللازمة، ودمج متطلبات أمن المعلومات ضمن عمليات المصرف، وتعزيز ثقافة أمن المعلومات والمسؤولية المشتركة لدى جميع العاملين والأطراف ذات العلاقة.

1. نطاق تطبيق السياسة

تسري هذه السياسة على نطاق نظام إدارة أمن المعلومات المعتمد في المصرف، وعلى جميع الإدارات والأقسام والفروع والعاملين والمتعاقدين والأطراف ذات العلاقة الذين يتعاملون مع المعلومات والأصول الواقعة ضمن نطاق النظام.

2. إدارة المخاطر وأمن المعلومات

يعتمد المصرف منهجاً قائماً على المخاطر في إدارة أمن المعلومات، من خلال تحديد وتقييم ومعالجة المخاطر المرتبطة بالمعلومات والأنظمة والخدمات والعمليات، واتخاذ الضوابط المناسبة للحد من المخاطر إلى المستويات المقبولة والمعتمدة، وفق منهجية إدارة مخاطر أمن المعلومات المعتمدة في المصرف.

3. الالتزام بضوابط الملحقAnnex (A)

يلتزم المصرف بتحديد وتطبيق ضوابط أمن المعلومات الواردة في الملحق (A) من المواصفة الدوليةISO/IEC 27001:2022 ، استناداً إلى نتائج تقييم ومعالجة مخاطر أمن المعلومات، والمتطلبات القانونية والتنظيمية والرقابية والتعاقدية المنطبقة، وطبيعة أنشطة المصرف واحتياجاته الأمنية والتشغيلية.

4. أهداف أمن المعلومات

تُعد هذه السياسة إطاراً لوضع ومراجعة أهداف أمن المعلومات بما يتوافق مع أهداف المصرف الاستراتيجية ونتائج تقييم المخاطر والمتطلبات المنطبقة واحتياجات الأطراف ذات العلاقة، على أن تكون الأهداف قابلة للقياس والمتابعة، ومسندة إلى الجهات المسؤولة عنها، وتتم مراجعة نتائجها بصورة دورية واتخاذ الإجراءات اللازمة عند وجود انحرافات أو تغييرات جوهرية.

5. إدارة الحوادث والاستجابة لها

يلتزم المصرف بتحديد وتوثيق والإبلاغ عن حوادث أمن المعلومات والاستجابة لها ومعالجتها وفق الإجراءات المعتمدة، واتخاذ الإجراءات اللازمة للحد من آثارها واستعادة الخدمات المتأثرة، والتنسيق مع الجهات ذات العلاقة عند الحاجة، والاستفادة من نتائج الحوادث والدروس المستخلصة في تعزيز الضوابط وتحسين نظام إدارة أمن المعلومات.

6. المسؤوليات والمساءلة

تتحمل الإدارة العليا مسؤولية اعتماد هذه السياسة وتوفير الموارد والدعم اللازمين ومتابعة فاعلية نظام إدارة أمن المعلومات، ويتولى مسؤول أمن المعلومات الإشراف على تطبيق النظام ومتابعة أداء وفاعلية الضوابط ذات العلاقة، فيما تلتزم الإدارات والأقسام والفروع بتطبيق متطلبات أمن المعلومات ضمن نطاق مسؤولياتها، ويلتزم جميع العاملين والمتعاقدين والأطراف ذات العلاقة بالسياسات والإجراءات والضوابط المعتمدة والإبلاغ عن أي حادث أو اشتباه بحادث أمني.

7. التوعية والنشر والإتاحة

يعمل المصرف على نشر وتعزيز الوعي بأمن المعلومات، وإتاحة هذه السياسة للعاملين والجهات ذات العلاقة وفق الوسائل المعتمدة، وحفظها كمعلومات موثقة ضمن نظام إدارة الوثائق المعتمد، مع المحافظة على التحكم بإصداراتها وتعديلاتها.

8. التحسين والمراجعة

تلتزم الإدارة العليا بالتحسين المستمر لفاعلية نظام إدارة أمن المعلومات من خلال متابعة الأهداف والمؤشرات، ونتائج تقييم المخاطر والتدقيق الداخلي والخارجي ومراجعات الإدارة وحالات عدم المطابقة والحوادث الأمنية، وتُراجع هذه السياسة مرة واحدة سنوياً على الأقل أو عند حدوث تغييرات جوهرية في نطاق النظام أو المخاطر أو المتطلبات القانونية والتنظيمية أو توجهات المصرف، وتُوثق جميع التعديلات والاعتمادات وفق نظام إدارة الوثائق المعتمد.

مصادقة المدير المفوض

علي محمد حسن العاملي