سياسة أمن وحماية المعلومات

المقدمة

هذه السياسة تدعم استراتيجية المعرفة لأن سياسة أمن وحماية المعلومات تتضمن تخزين المعلومات و توفير الحماية اللازمة للمعلومات ومنع الوصول إليها وهدرها من غير ذوي الصلاحية، وحمايتها من أيّ تهديد ، وتشمل هذه السياسة الأدوات والطرق والإجراءات اللازمة و الواجب توفرّها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل والخارج.

الهدف من وضع سياسات أمن وحماية المعلومات

١- الحفاظ على سلامة البيانات والمعلومات من العبث من قبل أشخاص غير مخولين. ابقاء البيانات والمعلومات تحت السيطره المباشرة والكاملة دون امكانية الوصول أو التعديل إلا من قبل الأشخاص المخول لهم ذلك.

٢- تحديد الأطر الأساسية لإجراء العمل.

٣- تحديد الأدوار والمسؤليات والواجبات العامة.

وتشمل سياسة امن وحماية المعلومات في مؤسسة الإقراض الزراعي ما يلي:

١- سياسة أمن و حماية المعلومات.

٢- سياسة الاستعمال المقبول.

٣- سياسة النسخ الاحتياطي (Backup).

سياسة أمن وحماية المعلومات

الهدف

الحفظ الآمن والسليم للمعلومات والبيانات في المؤسسة.

تفاصيل السياسة

تتبع المؤسسة سياسة واضحة لحفظ المعلومات من خلال اعتبار مديرية الحاسوب والمعلومات هي المديرية المسؤولة عن حفظ المعلومات و المديريات التالية : (مديرية الشؤون المالية والمصرفية ، مديرية الموارد البشرية ، مديرية خدمة الجمهور و قسم الديوان) مخزن للمعلومات والبيانات والوثائق، حيث تقوم هذه المديريات بدور كبير.

– وثائق تخص ملفات المقترضين في مديرية خدمة الجمهور:

يتم في قسم خدمة الجمهور تصنيف الوثائق بناءً على أرقام تسلسلية تعطى للمقترضين ويكون هنالك رمز code لكل فرع وجميعها تحفظ في تلك الملفات وفي خزائن للحفظ الأمين ومستودعات معده لذلك ، حيث تم استخدام نظام (Document Management System) الذي يتضمن نظام أرشفة وادارة سير الوثائق Document work flow وذلك للقيام بتبادل الوثائق بين الفروع والاداره وحفظها كنسخة الكترونية.

– البيانات والمعلومات التي يتم حفظها واسترجاعها من خلال نظام (ARBS) :

تقوم المؤسسة باستخدام أنظمة خاصة بأعمالها (ARBS) بتقنية الانترنت web enabled وتستخدم قاعدة بيانات مركزية ORACLE . وهذا مصمم على شكل حزم متكاملة ومترابطة ، وبصورة مرنة ، ضمن نظام أمن وحماية وصلاحيات على مستوى العمليات في الفروع وادارات الاقاليم والادراة العامة .

وهذه الأنظمة تحفظ البيانات والمعلومات التالية:

١– حسابات ومعلومات المقترضين والقروض الزراعية من طلبات قروض أو تمويل ، سندات الدين أو عقود التمويل ، والبيانات المالية الخاصة بها.

٢– المحاسبة العامة.

٣– التقارير والاحصائيات والمؤشرات المالية .

٤- الاقتطاعات حيث يتم التعامل مع بيانات الاقتطاعات الواردة من الدوائر الأخرى بصيغة الكترونية وربطها مع ملفات المقترضين.

٥- اللوازم والمستودعات .

٦- شؤون الموظفين والرواتب .

٧- القروض الخارجية .

٨- صندوق الادخار والاسكان.

ومن الممكن استرجاع أي بيانات أو وثائق مما سبق أعلاه كما ويستطيع الموظف المعني في أي مديرية الدخول على تلك الأنظمة لإسترجاع أي معلومة وحسب الصلاحيات المعطاه له وحسب طبيعة عمله والمعلومة التي يريدها .

- الوثائق التي تخص موظفي المؤسسة تختص بها مديرية الموارد البشرية:

أ- الآليات التي تتبعها مديرية الموارد البشرية لامتلاك البيانات والمعلومات وتخزينها بما فيها الوثائق الصادرة وذلك كما يلي:

١. الأنظمة والقوانين والتعليمات والتعاميم كما هي محفوظة حتى تاريخة.

٢. حفظ كل ما يصدر عن ديوان الخدمة المدنية وما يخص الموارد البشرية .

٣. حفظ كل ما يصدر من قرارات عن لجنة شؤون الموظفين.

٤. حفظ المعلومات الوظيفية مثل درجة الموظف أو فئته من الأوراق الرسمية الصادرة عن المؤسسة مثل كتاب التعيين أو براءة التشكيلات وتعتبر المرجع الرئيسي للمعلومات عن أي موظف.

٥. هناك نظام حاسوب خاص للموارد البشرية ضمن نظام ARBS يتم إدخال معلومات الموظفين الشخصية والوظيفية (بطاقة لكل موظف) والتي سبق ذكرها ويتم متابعتها على النظام حسب الأصول.

٦. تم البدء بنظام أرشفة ملفات الموظفين بالتنسيق مع ديوان الخدمة المدنية.

٧. يستطيع الموظف الإطلاع على البيانات الوظيفية من تاريخ التعين بواسطة البطاقة الإلكترونية المعتمدة مع ديوان الخدمة المدنية.

ب_ نظام التوثيق وحفظ البيانات: يعتبر نظام إدارة الموارد البشرية ضمن نظام ARBS المرجع

الرئيسي في معلومات الموظفين حيث يوجد لكل موظف ملف شخصي ورقي يدوي وملف الكتروني محوسب يشمل كافة معلومات مثل (الاسم الأول ، إسم الأب ، إسم الجد ، العائلة ، تاريخ ، مكان الميلاد ، تاريخ التعيين ، الحالة الاجتماعية ، المؤهل العلمي، الإجازات بكافة أنواعها ، العقوبات التي حصل عليها ، الدورات ، والراتب الأساسي) وكل ما يخص الموظف من معلومات ويعتبر النظام مرجع للموظف في حاله فقد أي من أوراقه الشخصية الخاصة دون الحاجة للرجوع إليه بحيث يتم متابعة هذا الموظف من خلال ملفه وليس شخصه فهو نظام توثيق مدعم للنظام الورقي والملفات الورقية القابلة للتلف أو الضياع أو الفقدان.

ج _ كيفية الوصول إلى البيانات والوثائق: يتم استرجاع معلومات الموظفين عن طريق تقارير تم تصميمها للحصول على البيانات المطلوبة ضمن محددات معينة لتحديد البيانات التي سيتم استعراضها على الشاشة في مديرية الموارد البشرية أو سحبها على الورق من خلال الاستعلام عن طريق رقم الموظف كمفتاح رئيسي لبيانات الموظف .

- بيانات ووثائق عامة تخص قسم الديوان:

يتولى توزيع الوثائق التي تخص المراسلات (صادر، وارد) موظفي قسم الديوان وذلك عند صدورها أو ورودها من وإلى المديرية العامة على شكل بريد بناءً على خبرة ومعرفة كافية من الموظفين بحيث يتولى موظفو القسم توثيق الوثائق على السجلات الخاصة بها، وتعطى رقم متسلسل وتاريخ وارد أو صادر ثم تحفظ وتحول إلى الجهات المعنية كل حسب اختصاصه بعد تصنيفها في الملفات الخاصة بها، ويتم استرجاع البيانات والمعلومات والوثائق عند طلب إي معلومة عن طريق تحديد الموضوع أو اسم صاحب العلاقة سواء كان (موظف أو مقترض) ومن خلال فهارس وأدلة محدده يتم استرجاع الملف الذي يحتوي الوثيقة المطلوبة.

كيفية ضمان أمن وحماية البيانات والوثائق الخاصة بالمقترضين :

فيما يتعلق بأمن وحماية البيانات يتم أخذ نسخة احتياطية من البيانات المخزنة على جهاز الحاسوب على أقراص ممغنطه أولاً بأول ويتم الإحتفاظ بأكثر من نسخة من هذه الأقراص إضافة الى ذلك يتم تخزين البيانات على الجهاز الرئيسي SERVER كجزء من عملية حماية للبيانات.

وتعتمد المؤسسة على عدة أساليب لحفظ وحماية وثائقها بالإضافة إلى ما سبق ذكره من مستودعات الحفظ الأمين مثال ذلك :-

١- إصدار نسخه إضافية عن أي وثيقة صادرة يتم حفظها بالملف.

٢- حفظ الوثائق القديمة والملفات التي ليس عليها إجراءات منتظمة والتي يندر استرجاعها في مستودع كبير كان في السلط . تم تشكيل لجنه لأخذ القرار في الملفات التي لا تستعمل وتم اعادة تدوير عدد كبير من الملفات وتحويل الملفات التي مازال عليها اجراءات الى فرع الزرقاء لانه يوجد مستودع كبير هناك محمي وأمين ومنظم بسجلات وأدله خاصة.

٣- توفر مستودع خاص بالوثائق والأوراق المالية يتبع للإدارة المالية ويوجد به موظفين مختصين بإدارة وحفظ وحماية واسترجاع هذه الوثائق من ضمنها ملفات تعود لمقترضي الضفة الغربية قبل عام ١٩٦٧.

٤- توفر نسخة من ملف المقترض بالفرع وأخرى في مستودع إدارة الأقاليم الذي يتبعه الفرع ونسخة ثالثة في المديرية العامة علماً بان المحتوى لهذه الملفات مطابق لكافة الوثائق والنسخ ويتم استرجاع هذه الوثائق من خلال رقم المقترض الموحد في المستودعات الثلاث.

٥- يوجد ملف خاص بموظفي المؤسسة مكتوم يتم تداوله من قبل الإدارة العليا فقط .

سياسة الاستعمال المقبول

الهدف

توفير بيئة آمنة وموثوقة بحيث يتحمل جميع العاملين في المؤسسة المسؤولية في الاستعمال الصحيح للمعلومات ومواردها والبنية التحتية التكنولوجية لها.

تفاصيل السياسة

تضمن مديرية الحاسوب والمعلومات أمن وسرية الموجودات والمعلومات من خلال الإجراءات والأدوات المستخدمة لحماية الأنظمة والمعلومات وذلك من خلال مايلي :

١- تجهيزات موقع الأجهزة الرئيسي: Security access door، Raised Floor، Automatic fire and alarm system، Uninterrupted power supply system (UPS)، Cooling systems .

٢-خطوط الإتصال: تستخدم المؤسسة تقنية مايكروويف MPLS لربط كافة الفروع مع موقع الادارة وتقنية الألياف الضوئية من جهة الإدارة ، وفي حال الإنقطاع من جهة الفروع يتم التحويل إلى خطوط ADSL وذلك لضمان استمرارية الإتصال ، كذلك يوجد عدة خطوط "فايبر" من طرف موقع الإدارة يتم توزيع ربط الفروع فيها ، وفي حال تعطل أو انقطاع احد تلك الخطوط يتم التحويل الى خط آخر مباشرة .

- الحماية على الشبكة والأجهزة:

٣- سابقاً كان يتم استخدام (ISA 2004 + CISCO PIX firewall and fail over firewall Firewall) و الآن تم استبدالها وتحديثها الى (Cyperoam next Generation) firewall

Domain Control Policy Kaspersky Antivirus and Anti span on e-mail server managemen

٤- الحماية على الأنظمة المستخدمة

Windows Domain User/password management

Oracle database User/password management

Application embedded security management

١- إستخدام أجهزة الحاسوب في المؤسسة

- الممارسات المسموح بها

١- يتم تثبيت (installation) وتركيب وتحديث البرمجيات المرخصة والخاصة بالعمل عن طريق مديرية الحاسوب والمعلومات فقط.

٢- تستخدم البرمجيات المرخصة فقط ، لتحقيق أهداف المؤسسة والأعمال المناطة به .

- الممارسات الممنوعة:

التي يتم مراقبتها ومتابعتها من قبل مديرية الحاسوب والمعلومات. فقد أصدر أكثر من تعميم (لاحقاً للتعاميم ذوات الأرقام (٩) تاريخ ٢٠١١/٥/٢٣ و (١٦) تاريخ ٢٠١١/٧/١٣ و (١٣) تاريخ ٢٠١٢/٥/٢١)

آخر التعاميم رقم (٩) تاريخ ٢٠١٥/٧/٢٩ وكان يتضمن ...

أرجو أن أوكد عليكم ضرورة التقيد بما يلي:

١- استخدام خدمة الإنترنت والبريد الالكتروني الخاص بالمؤسسة فقط لغايات العمل الرسمي.

٢- عدم استخدام Internet Flash الشخصية الخاصة بالموظف على أجهزة المؤسسة.

٣- عدم تحميل أية برمجيات لم يتم اعتمادها من قبل مديري الحاسوب.

٤- عدم استخدام رمز المستخدم للموظف من قبل موظف اخر على نظام ARBS أو صلاحيات استخدام الشبكة.

٥- عدم تخزين ملفات شخصية على أجهزة المؤسسة.

كما يمنع :

١- فتح أو محاولة صيانة اجهزة الحاسوب (سواء من قبل المستخدم او طرف من خارج المؤسسة) دون الرجوع لمديرية الحاسوب والمعلومات .

٢- فك ونقل اجهزة الحاسوب دون الحصول على موافقة الإدارة العليا او مديرية الحاسوب والمعلومات.

٢- استخدام الإنترنت في المؤسسة

يتم فلترة المواقع المستخدمة في المؤسسات الحكومية من قبل مركز المعلومات الوطني، بناء على توجيهات حكومية عليا تهدف الى تفرغ الموظفين لخدمة المواطن . كما يتم فلترة مواقع الانترنت من قبل مديرية الحاسوب والمعلومات في المؤسسة (Next Generation Fire wall) .

٣- استخدام شبكة الحاسوب في المؤسسة

١- استخدام أجهزة وعناصر الشبكة والبنية التحتية المعلوماتية لأغراض العمل الرسمي.

٢- تثبيت (installation) وتحديث وضبط إعدادات البرمجيات Domain Controller.

٣- منح و حجب الصلاحيات حسب الوصف الوظيفي للمستخدمين ، (منح الصلاحيات على

انظمة المؤسسة هي عملية إعطاء الموظفين قدرات أوسع أو (سلطة) لممارسة التحكم وتحمل مسؤولية عملهم في المؤسسة بما يتناسب مع طبيعة عمل الموظف /الموظفة مثل (ادخال البيانات، تعديل ، ترحيل، استعلام ، طباعة تقارير وغيرها).

٤- استخدام البريد الالكتروني في المؤسسة

يتم العمل على توفير البريد الالكتروني Outlook في المؤسسة للموظفين من أجل فتح وقراءة وإرسال وتخزين البريد الالكتروني الرسمي.

سياسة النسخ الاحتياطي (Backup)

الهدف

ضمان استمرارية توفر البيانات على أجهزة الحاسوب في المؤسسة.

تفاصيل السياسة

النسخ الاحتياطية للبيانات والأنظمة: يتم عمل نسخ إحتياطية من قبل التشغيل والدعم الفني حسب البرنامج التالي:

Location	Type	Period
Server room غرفة الأجهزة	Data base export Database backup to DVD	Daily backup
القاصة الخاصة في الإدارة الرئيسية	Data base export Database backup to DVD	Weekly backup
القاصة الخاصة في الإدارة الرئيسية	Data base export Database backup to DVD	Monthly backup

القاصة الخاصة في الإدارة الرئيسية	Data base export Database backup to DVD	Yearly backup
مديرية الحاسوب والمعلومات	Depending on event	Major event backup