سياسة تقنية المعلومات

مقدمة

تعتبر السياسات في أي منظمة العمود الفقري في تسيير أعمالها بين وحداتها الإدارية الداخلية ومع الجهات الخارجية، ومع الجمهور من المستفيدين، الموردين، وغيرهم، ولذلك تولي المنظمات على مختلف أنشطتها اهتماماً كبيراً بتطبيق السياسات لما لها من أثر فعال على كفاءة الأداء وتحقيق الأهداف التنظيمية.

ومن هذا المنطلق؛ جاء اهتمام المؤسسة بإعداد عدد من السياسات وذلك لتحقيق المستهدفات في مجالات عملها والتكامل مع الجهات الرقابية المختصة، من خلال اتباع معايير واضحة للمسؤولية في جميع المستويات التنفيذية للتقيد بالسياسات والخطط والأنظمة واللوائح المعتمدة، وايجاد تنظيم يعمل على توحيد الممارسات في تطبيق الالتزامات النظامية وإتباع الممارسات الرائدة في مجال الحوكمة بهدف التميز في الأداء والاستمرارية والاستدامة في الأعمال ويساعد على تحقيق رسالة المؤسسة، ومنها " **سياسة تقنية المعلومات**".

سياسة تقنية المعلومات

الاستخدام المقبول لموارد التقنية

- موارد المؤسسة التقنية هي مصدر محدود بإمكانياته (مثال، الانترنت – مساحة التخزين – الطابعات)، ولهذا فإنه يترتب على المستخدم أخلاقياً استخدامها بطريقة عادلة تحترم حقوق وحاجات المستخدمين الآخرين، حيث أن الاستخدام يكون لأغراض البحث والعمل اليومي الخاص بالمؤسسة.
- تُعتبر الحواسيب والشبكات ونظم المعلومات الإلكترونية موارد أساسية لتحقق المؤسسة رسالتها التي أنشأت من أجلها وتقديم الخدمة لموظفيها والمستفيدين بما يتوافق مع احتياجاتهم وتطلعاتهم وتمنح المؤسسة منسوبيها حق الولوج إلى هذه الموارد بغية دعم تحقيق رسالتها.
- تُعدّ هذه الموارد أصول قيمة للمؤسسة وينبغي استخدامها وإدارتها على نحو مسؤول لضمان أمنها وسلامتها وإتاحتها للأنشطة المناسبة، وعلى كافة مستخدمي هذه الموارد أن يستخدموها بشكل مسؤول وفاعل.
- لا تستخدم البيانات/المعلومات والنظم إلا من قبل الأشخاص المخول لهم استخدامها للقيام بمهام تتعلق بأداء أعمالهم، ويمنع استخدام المعلومات والنظم لمكاسب أو أعمال شخصية أو لارتكاب أعمال الغش.
- يمنع المستخدم منعاً باتاً من محاولة استخدام خدمات غير مصرح له، أو القيام باستخدام أي برنامج مشبوه يؤثر سلباً على موارد المؤسسة كونه مصدر للفيروسات مثلاً، أو أي برنامج حاسوبي أو معلومات تقنية أو برامج تشفير بما يخالف قوانين هذه الوثيقة أو قوانين الحماية المحلية أو الدولية.
- يتحمل المستخدم المسؤولية كاملة عن جميع البيانات والملفات الموجودة على جهاز الحاسوب الخاص به، حيث يقع على عاتقه مسؤولية الحفاظ عليها وعمل نسخ احتياطي لها في مكان آخر آمن مثل النسخة السحابية الموفرة، كذلك يلتزم المستخدم بعدم مشاركة الآخرين بالمعلومات أو الملفات الحساسة التي توجد على الجهاز الخاص به.
- يحظر على المستخدمين الافصاح أو الكشف عن أية معلومات دون تفويض أو تخويل رسمي، ويشكل الولوج غير المسموح به للمعلومات أو التلاعب بها أو الإفصاح عنها أو تسريبها دون أخذ الصلاحية خرقاً أمنياً قد يؤدي إلى اتخاذ عمل تأديبي والملاحقة القضائية من قبل الجهات الحكومية.
- الأجهزة المملوكة للمؤسسة:
  - الأجهزة المقدمة من المؤسسة يجب أن تفي بالحد الأدنى من متطلبات الأمن، وبالإضافة إلى ذلك ما يلي:
    - ⇐ عدم إجراء أي تغيير غير مصرح به في الأجهزة المقدمة من المؤسسة.
    - ⇐ إرجاع الأجهزة للمؤسسة في حالة عدم الحاجة اليها.
  - أنظمة التبريد داخل الداتا سنتر عبارة عن عدد ٢ جهاز تكييف اسبليت حديثة، درجة حرارة التبريد ١٦-١٩ درجة مئوية، تعمل بنظام التبادل لمدة ١٥ يوم يتم تشغيل جهاز واغلاق الاخر.
  - هناك قائمة بالموارد التقنية المتاحة للإستعارة، عند الحاجة لأحد هذه الموارد الرجاء التكرم بارسال بريد لإدارة التقنية it@asf.org.sa موضحاً الآتي:
    - ⇐ المورد المراد استعارته.
    - ⇐ الغرض من الاستعارة.
    - ⇐ مدة الاستعارة (متى تبدأ ومتى تنتهي).

كلمة المرور

- تُعدّ كلمات المرور جانباً هاماً في أمن الحواسيب، كما تعُدّ خط الدفاع الأول لحماية حسابات المستخدمين، إذ قد تتسبب كلمة المرور المنتقاة بشكل سيء في إلحاق الضرر بكامل الشبكة.
- وتُعدّ كلمة المرور التي لا تنتهي صلاحيتها على الإطلاق من المخاطر لأنها قد تتعرض للكشف مع مرور الوقت
- تقع على عاتق جميع منسوبي المؤسسة مسؤولية اتخاذ الخطوات المناسبة لاختيار كلمات مرورهم بشكل آمن.
- يحق لجميع منسوبي المؤسسة الحصول على اسم مستخدم وكلمة مرور يسمح من خلاله الاستفادة من الأنظمة والخدمات المرتبطة بالشبكة.

- يجب التعامل مع كلمات المرور كافة بوصفها معلومات حساسة وسرية في المؤسسة.
- تحدد شكل كلمة المرور على الاتي:
  - الحد الأدنى من طول كلمة المرور من **8** أحرف،
  - يجب أن تحتوي كلمة السر على الفئات التالية:
    - ⇐ أحرف كبيرة باللغة الإنجليزية مثل (A, B, C, ... Z)
    - ⇐ أحرف صغيرة باللغة الإنجليزية مثل (a, b, c, ... z)
    - ⇐ أرقام عددية من 0 إلى 9
    - ⇐ رموز خاصة) مثل (.,!() :"%#@*^) (اختياري)
  - يتاح للمستخدم تكرار كلمة المرور القديمة بعد إدخال ٤ كلمات مرور.
  - يجب أن لا تكون كلمات المرور يسهل تخمينها " أسماء أي من أشهر السنة، وأيام الأسبوع، واسم المستخدم".
- تفعل سياسة كلمة المرور بشكل تلقائي.
- لا يتم إنشاء حساب إلا بقرار موافقة عمل من إدارة الموارد البشرية.
- عندما يتقدم المستخدم بطلب لإعادة ضبط كلمة المرور فإن ذلك يتطلب التحقق من شخصية المستخدم.
- في حالة نسيان الموظف لإسم المستخدم أو كلمة المرور فإن على الموظف فتح طلب وتزويد إدارة التقنية بصورة من بطاقة العمل للتأكد من بيانات الموظف.
- يحق لجميع منسوبي المؤسسة طلب تغيير كلمة المرور للحساب الخاص في حال نسيانه أو عدم القدرة في الدخول لأي سبب كان؛ التعديل لا يشمل تغيير اسم المستخدم بأي حال من الأحوال.
- يجب أن تتوافق كلمات المرور الخاصة بالمستخدمين مع المعايير القياسية المدرجة أدناه.
- صلاحية كلمة المرور ٩٠ يوم، ويجبر النظام المستخدم على تغييرها بعد انقضاء تلك المدة، مع إمكانية تغيير كلمة المرور بشكل اختياري خلال تلك المدة.
- عدد محاولات الدخول الفاشلة لحساب المستخدم ٥ محاولات قبل أن يؤمن الحساب.
- فترة تأمين الحساب تستغرق ٣ دقائق انتظار قبل إعادة الفتح.
- يتم تفعيل/ تغيير كلمة المرور عند الدخول القادم لإعادة الضبط، أو تفعيل كلمات مرور الحسابات الجديدة.
- يجب ألاّ يتم توقيع إخلاء طرف الموظف المستقيل أو المنتهية خدمته من قبل إدارة التقنية إلاّ بعد حذف أسمه والتأكد من عدم إمكانية دخوله نظام المعلومات.

الإنترنت

- إن الغرض الأساسي من توفير الإنترنت في المؤسسة هو تمكين موظفيها من الاستفادة من التسهيلات التي يقدمها في مجال الاتصالات والمعلومات اللازمة لأداء المهام والواجبات الرسمية.
- يحق لجميع منسوبي الشركة والزوار الحصول على خدمة الانترنت.
- جميع الموظفين لديهم المسؤولية لاستخدام الانترنت بطريقة مهنية أخلاقية وقانونية.
- ينبغي على موظفي المؤسسة الالتزام باستعمال الإنترنت لأغراض العمل فقط والامتناع عن استخدامه لأغراض شخصية أثناء وقت الدوام الرسمي.
- يجب على المستخدمين توخي الحذر عند استخدام المدفوعات عبر الانترنت من المواقع التي تقوم بالاحتيال لطلب أرقام سرية خاصة بالبطاقات الائتمانية، " مؤسسة عبدالله السبيعي الخيرية" ليست مسؤولة عن الخسائر الناجمة عن طريق نقل البيانات السرية للبطاقات الائتمانية أو المعلومات الشخصية عبر الانترنت.
- الانترنت مصدر محدود بإمكانياته، ولهذا فإنه يترتب عليه أخلاقياً استخدامه بطريقة عادلة تحترم حقوق وحاجات المستخدمين الآخرين ولا تستنفد معظم النطاق مثل مواقع عرض الفيديو والصوت ومراكز التحميل، حيث أن الاستخدام يكون لأغراض البحث والعمل اليومي الخاص بالمؤسسة.

- يجب على جميع المستخدمين الوصول إلى شبكة انترنت المؤسسة والتي تمر عبر القناة المعتمدة التي يتم تأمينها بجدار ناري للحماية من خلال أجهزة المؤسسة.
- يجب على المستخدمين عدم استخدام كلمات المرور المستخدمة داخل أنظمة من أجل الدخول إلى مواقع الإنترنت كما يفعلون في الداخل لأنظمة المؤسسة.
- المؤسسة غير مسؤولة عما يقوم به المستخدم على شبكة الإنترنت، وأنه المسؤول الوحيد بشكل كامل عن أي عمل يقوم به على شبكة الإنترنت، سواء بالتصفح أو الكتابة أو التحميل على شبكة الإنترنت.
- لا يجوز الدخول على مواقع أو صفحات الإنترنت المخلة بالآداب والقيم العامة أو عرض الصور أو الملفات المتوفرة فيها أو حفظها أو توزيعها أو تحريرها.
- لا يجوز لموظفي المؤسسة تحميل برامج التواصل الاجتماعي والترفيه والألعاب أو اللعب المباشر عن طريق شبكة الإنترنت.
- يتم متابعة استعمال الإنترنت للتأكد من حسن استخدامها وإعداد تقارير دورية بالنتائج.
- يعلم المستخدم أن للمؤسسة الحق في المنع الكلي أو الجزئي لبعض مواقع وخدمات الإنترنت التي تتعارض مع سير العمل أو أخلاقياته أو التي قد تؤثر سلباً على كفاءة شبكة الإنترنت وسرعتها في المؤسسة.
- يحق لجميع مدراء الوحدات الإدارية في الشركة التقدم بطلب إضافة أو إيقاف صلاحيات محددة للوصول للإنترنت لموظف في وحدته الإدارية.
- يتوجب على إدارة التقنية الاستفادة من كافة الوسائل المتاحة من برمجيات وغيرها لتنظيم عملية استخدام الإنترنت وفقاً للسياسات المعتمدة.
- توضح الجزاءات المناسبة للمخالفات الخاصة بسياسات وقواعد استعمال الإنترنت من قبل إدارة التقنية.

الشبكة اللاسلكية

- يتم الاحتفاظ بكافة عناوين الأجهزة (MAC) وتسجيلها إذا لزم الأمر .
- جميع نقاط الوصول اللاسلكية سيتم تثبيتها من قبل خدمات تقنية المعلومات في مواقع المؤسسة، مع توفير الدعم والصيانة لها.
- بروتوكولات التشفير المعتمدة ستكون قيد الاستخدام.
- الشبكة اللاسلكية تخدم أجهزة الجوال والأجهزة الذكية لمنسوبي المؤسسة والضيوف وتخدم أجهزة الكمبيوتر المحمول وهي موزعة في أربعة أماكن لتغطي كافة أرجاء المؤسسة.
- يجب أن تكون الأجهزة المتصلة على الشبكة اللاسلكية محمية بمكافح فيروسات، وإدارة التقنية غير مسؤولة عن أي أضرار تنتج عن تبادل البيانات بين الأجهزة المتصلة على الشبكة اللاسلكية.

الأجهزة والهواتف النقالة

- على المستخدمين اتباع وتنفيذ الضوابط الأمنية لأجهزة الهواتف النقالة للمؤسسة لتأمين البيانات المحمية والمخزنة في الهواتف النقالة. ويجب ألا يتم تخزين البيانات الهامة والحيوية دون تنفيذ ضوابط أمنية فعالة لحماية البيانات، وعلى المستخدمين استخدام خاصية التشفير أو تدابير فعالة في أجهزة الهواتف النقالة التي تحتوي على بيانات حيوية للمؤسسة وتشمل التدابير الفعالة الأخرى الحماية المادية التي تضمن وصول المخول لهم فقط للمعلومات المخزنة.

أمن المعلومات

- تعتمد المؤسسة على إتاحة وسلامة خدماتها الالكترونية، وفي إطار ذلك يكون من الضروري حماية نظم تقنية المعلومات والبنى التحتية من مخاطر أمنية سواء أكانت داخلية أو خارجية ومتعمدة أو عرضية.
- يعدّ جميع أعضاء المؤسسة مسؤولين عن الالتزام بمعرفة الآليات واللوائح التي تضمن ما يلي:
  - حماية المعلومات من أي وصول غير مسموح به.
  - سرية المعلومات.
  - الحفاظ على سلامة ومصداقية المعلومات.
  - الحفاظ على إتاحة المعلومات.

- تحقيق المتطلبات التنظيمية والتشريعية.
- تطوير خطة استمرارية العمل وفحصها والحفاظ عليها. (خطة مواجهة الأعطال للشبكات والأنظمة).
- إتاحة التوعية والتعريف بأمن المعلومات بالنسبة لمنسوبي المؤسسة.
- إبلاغ إدارة التقنية المعلومات عن كافة أشكال الخروقات الفعلية أو المحتملة لأمن المعلومات من أجل القيام بالإجراء اللازم وللتواصل من إدارة التقنية عبر البريد الخاص بالإدارة (**it@asf.org.sa**) أو الاتصال على رقم التحويلة الخاصة بالإدارة .
- إيجاد إجراءات من شأنها دعم هذه السياسة بما في ذلك إجراءات ضبط الفيروسات وكلمات المرور وخطط الاستمرارية.
- تحقيق متطلبات إتاحة النظم والمعلومات.
- عدم السماح لأي نوع من النظم الاتصال بالشبكة دون برنامج مكافحة الفيروسات.
- تحديث جميع برمجيات مكافحة الفيروسات من قبل خدمات تقنية المعلومات بانتظام، مع التحقق من الأنظمة.
- التحقق من أن جميع الملفات التي تم تحميلها عن طريق البريد الإلكتروني من مصدر موثوق به وخالية من الفيروسات.
- التحقق من مسح جميع الوسائط غير المثبتة من الفيروسات قبل الاستخدام من قبل المستخدم.

- يجب على إدارة التقنية المعلومات تزويد جميع الخوادم ببرامج مكافحة الفيروسات والتأكد أن كفاءتها ضد الفيروسات مضمونة.
- لا يسمح لأي مستخدم باستخدام شريحة ذاكرة في أجهزة الحواسيب المكتبية الخاصة به إلا بعد التحقق من خلوها من الفيروسات.
- يتم مسح (**scan**) جميع مراسلات البريد الإلكتروني الصادر والوارد للتأكد من خلوها من الفيروسات.
- يتم عزل رسائل البريد الإلكتروني المصابة والاحتفاظ بها في مكان معزول (**Quarantine**) مع إخطار المستخدم، وتقديم الحل الأمثل من خدمات تقنية المعلومات.
- يتم قفل حساب المستخدم المتضرر وفصل النظام المتضرر من الشبكة وعزله وتطويقه إلى أن يتم تطهيره من قبل خدمات تقنية المعلومات.
- يمنع فتح أو استكشاف أو إعادة توجيه للبريد الإلكتروني ذو المحتوى الضار أو المشكوك فيه من قبل الموظف دون تعليمات من قبل خدمات تقنية المعلومات.
- تعتبر" إدارة التقنية المعلومات " مسؤولة عن الحفاظ على هذه السياسة وعن تقديم الدعم والنصيحة أثناء تنفيذها.
- يمنع منعاً باتاً قيام المستخدم بنسخ أي من المواد التي تخضع لحقوق الطبع أو استخدام أية برامج غير مرخصة على أجهزة المؤسسة.
- تم تخصيص لكل موظف اسم مستخدم وكلمة مرور لا يجب الكشف عنها لشخص آخر. وسيكون صاحب الحساب مسؤول عن كافة الأعمال التابعة للحساب.
- لا يجوز ولا يحق لمستخدم شبكة المؤسسة القيام باستخدام معلومات حساب مستخدم آخر أو محاولة الحصول عليها أو تخمينها لاستخدام خدمات شبكة المؤسسة.
- إدارة التقنية المعلومات لا تحتفظ بكلمات السر كنص عادي يمكن قراءته، وإنما يتم حفظ كلمات السر على شكل نص مشفر لا يمكن فكه او استخدامه، وإنما يمكن تغيير كلمة السر بناء على طلب المستخدم وهو المسؤول عن تغييرها بعد ذلك.
- في حالة فقدان المعلومات السرية، يجب إبلاغ إدارة التقنية لتقديم المساعدة.
- في حالة الحاجة إلى جهاز حاسب محمول، يتم تقديم طلب للدعم الفني محدد المدة والغرض لإدارة التقنية، وحذف أي بيانات خاصة بعد فترة استخدامه.
- تؤمن إدارة التقنية أجهزة النسخ الاحتياطي المختلفة لكل إدارة لحفظ الملفات الهامة.
- يجب تأمين أجهزة الحاسب الآلي والأجهزة المحمولة أو تسجيل الخروج في حال الابتعاد عنها وعدم تركها.
- يمنع تحميل أي برامج أو إزالتها الا عن طريق إدارة التقنية بإشعار مسؤول الدعم الفني وهو الذي سيقوم بتلبية الطلب بعد دراسته.

- مكافح الفيروسات له مهام متعددة أي أنه "مكتشف ومكافح للفيروسات – ديدان البريد – مكافح لملفات التجسس – مضاد للاختراق – مكافح للبريد المزعج " من المهم أن يتأكد المستخدم من فاعليته وإبلاغ إدارة التقنية في حالة توقفه عن العمل أو انتهاء صلاحيته أو ملاحظة تقرير غير اعتيادي منه.
- صلاحية المستخدم على الجهاز صلاحية عادية تحفظ بذلك الجهاز وشبكة المؤسسة من كثير من التهديدات التي قد تسبب أضرار وتحد من تنزيل البرامج وتشغيل الملفات القابلة للتنفيذ **exe** ونحوها.
- لا يسمح للمستخدم تعطيل برنامج مكافح الفيروسات تحت أي ظرف من الظروف إلا بإشراف إدارة التقنية.
- إخلاء المسؤولية:
- اعتماد إجراء "إخلاء المسؤولية" وهو عبارة عن نص تتم إضافته تلقائيًا إلى رسائل البريد الإلكتروني الصادرة إلى خارج المؤسسة، ويكون موقعها في ذيل الرسالة أسفل التوقيع الشخصي، يتم استخدام إجراء إخلاء المسؤولية لتوفير غطاء قانوني وتحذيرات في حال تم وصول البريد إلى مستقبل غير مقصود، ويمكننا تحديد أي شروط يلزم تطبيقها على إخلاء المسؤولية. على سبيل المثال: اختيار تطبيق إخلاء المسؤولية على كافة الرسائل الموجودة في المؤسسة أو على الرسائل المرسلة إلى مستلمين خارجيين، ويمكن تحديد إجراء إخلاء مسؤولية مختلفة للمستلمين الداخليين والخارجيين أو للرسائل المرسلة من قبل مستخدمين في أقسام أو مكاتب معينة، والمطبق بالمؤسسة على كافة الرسائل المرسلة إلى مستلمين خارجيين. ونص العبارة المستخدم باللغتين العربية والإنجليزية كما يلي:

إخلاء مسؤولية: هذه الرسالة وما تحتويه تعني المرسل إليه وقد تحتوي على معلومات سرية أو خاصة. إن ما تمثله الرسالة من آراء تعبر عن وجهة نظر المرسل ولا تمثل بالضرورة وجهة نظر مؤسسة عبد الله السبيعي الخيرية. إن أي عملية اطلاع أو توزيع أو استخدام غير مصرح به يعتبر خرقا للقانون. إذا لم تكن المتلقي المقصود يرجى الاتصال بالمرسل فورا عن طريق البريد الإلكتروني والتخلص من جميع نسخ هذه الرسالة

Disclaimer: *This e-mail message and any attachments are for the sole use of the intended recipient(s) and may contain proprietary, confidential or privileged information. Any views or opinions expressed are solely those of the author and do not necessarily represent those of Subeaei Charity Foundation. Any unauthorized review, use, disclosure or distribution is prohibited and may be a violation of law. If you are not the intended recipient, please contact the sender immediately by reply e-mail and destroy all copies of this message.*

- عزل النظم الحساسة:

قد يتطلب النظم الحساسة (الخارجية) بيئة حاسوبية منفصلة، وقد تشير الحساسية إلى وجوب تشغيل النظام في خادم منفصل وخارج نطاق الشبكة الداخلية للموظفين، ويتم اتخاذ قرار عزل أي نظام بناءً على قرار من فريق إدارة التقنية. يتم العزل عن طريق التقنيات المتوفرة مثل تقنية الـDMZ .

إدارة البيانات

تصنيف البيانات:

- تعتبر موارد المعلومات في المؤسسة بالغة الأهمية بالنسبة لعمليات المؤسسة، وقد وضعت سياسة تصنيف البيانات هذه بغرض حماية بيانات المؤسسة والتقليل من أي مخاطر قد تؤثر سلباً على عمل المؤسسة أو على قدرتها في أداء مهمتها. وتعتبر سياسة تصنيف البيانات طريقة للتعرف على مستويات البيانات من ناحية حساسيتها ومخاطرها.
- تلتزم إدارة الموارد البشرية بأخذ الإجراءات القانونية اللازمة لضمان إلتزام الموظفين بعدم إفشاء المعلومات والبيانات التي تخولهم وظائفهم الوصول إليها، وذلك عن طريق توقيع "إتفاقية سرية البيانات".
- يتم تصنيف بيانات المؤسسة في أي نظام إلى أربع مستويات:
  - بيانات سرية وهي بيانات عالية الحساسية، وقد يشكل الكشف عن مثل هذه البيانات أثر سلبي على المؤسسة، وينبغي تطبيق أقصى مستويات التحكم في هذه البيانات. من أمثلة هذه البيانات، المعلومات المالية ومعلومات الموظفين الشخصية ومفاتيح تشفير الملفات.
  - بيانات خاصة وهي بيانات متوسطة الحساسية، قد يضر الكشف عن هذه البيانات عمليات المؤسسة، ولا تحتوي هذه البيانات على معلومات سرية. من أمثلة هذه البيانات التقارير الداخلية وبعض المعاملات المالية.
  - بيانات حساسة (للاستخدام الداخلي فقط) وهي بيانات لا يجوز نشرها خارج إطار المؤسسة. تعتبر هذه البيانات ذات مخاطر منخفضة وذلك لأن نشرها لا يضر بالمؤسسة. من أمثلة هذه البيانات محاضر الاجتماعات والمذكرات الداخلية وخطط العمل والتقارير الداخلية للمشاريع.

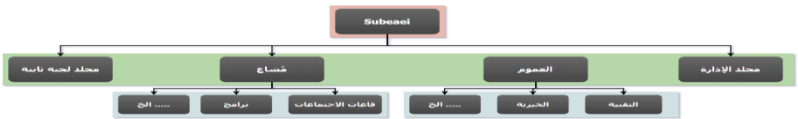
- البيانات العامة وهي أية بيانات يمكن للعامة الوصول إليها، ويكون للكشف عن هذه البيانات أثر إيجابي أو محايد على المؤسسة. أمثلة هذه البيانات الأخبار والفعاليات الخاصة بالمؤسسة والتقارير السنوية ومعلومات التقديم ومطبوعات المؤسسة.

- تقع مسؤولية تصنيف البيانات على عاتق المسؤول عن تلك البيانات كل في مجال عمله، ويتعين على المستخدمين المخول لهم الوصول لتلك البيانات أن يتحققوا من تصنيف البيانات من المسؤول عنها قبل مشاركتها داخلياً أو خارجياً.
- مدراء الوحدات الإدارية مسؤولون عن مراجعة وتقييم وتصنيف البيانات التي تقع تحت مسؤوليتهم وذلك بالتنسيق مع الفريق التقني للمؤسسة.
- مسؤولي الأنظمة مسؤولون عن التنسيق مع مديري الوحدات الإدارية وذلك للمساعدة في تطبيق إجراءات ضبط وتصنيف البيانات وفق التعريف السابق.
- المستخدمون النهائيون مسؤولون عن استخدام البيانات تبعاً للتعريفات والتصنيفات التي يحددها أمناء المعلومات (مديري الوحدات الإدارية + إدارة التقنية).

تصنيف البيانات:

- هيكلية وتقسيم الخادم:

تم تقسيم الخادم بطريقة تلبي الاحتياج وتتيح الخصوصية للوحدات الإدارية والأفراد وفيها مرونة وسرعة في تبادل الملفات، ويختلف ظهور الملفات لكل شخص حسب الصلاحيات الممنوحة له بناء على إدارته والمهام التي يقوم بها على النحو التالي:



- المجلد الرئيسي (**Subeaei**):
  - ⇐ بالامكان الوصول له عن طريق أيقونة جهاز الكمبيوتر
  - ⇐ تظهر مجلدات المشاركة الخاصة بكل موظف بشكل تلقائي على حسب صلاحياته
- مجلد الإدارة:
  - ⇐ هو مجلد خاص للإدارة يتم تقسيمه وتوزيع صلاحياته على حسب حاجة كل إدارة.
  - ⇐ لا يمكن لأي إدارة رؤية مجلد الإدارة الأخرى.
  - ⇐ المساحة الافتراضية لكل إدارة هي GB 10.
- مجلد العموم:
  - ⇐ هو مجلد مخصص للإدارة التي لديها ملفات يحتاج عموم الموظفين الإطلاع عليها.
  - ⇐ يتم اختيار شخصين من قبل الإدارة لعملية إدارة محتوى المجلد.
  - ⇐ المساحة الافتراضية لكل إدارة GB 5.
- مجلد مشاع:
  - ⇐ هو مجلد الجميع له صلاحية القراءة والكتابة عليه لمشاركة الملفات فيما بينهم.
  - ⇐ يوجد داخله مجلد خاص بقاعات الاجتماعات لتبادل الملفات بين أجهزة الموظفين وأجهزة القاعات.
  - ⇐ للجميع صلاحية الإضافة والحذف.
  - ⇐ المساحة الافتراضية GB 50.
  - ⇐ يتم تنظيفه ومسح محتوياته بشكل دوري، ولا يؤخذ له نسخة احتياطية.
- اللجان الثابتة:
  - ⇐ مجلد خاص بأي لجنة ثابتة تحتاج مساحة فيما بينهم مثل فريق المؤسسة.

- ⇐ عند الحاجة لاستحداث مجلد جديد يتم التواصل مع إدارة التقنية.
- ⇐ المساحة الافتراضية 5 GB.
- ⇐ عند الحاجة لزيادة المساحة لأي مجلد التقدم بطلب لإدارة تقنية المعلومات لدراسته وتنفيذه.

- يتم أخذ نسخة احتياطية بشكل دوري أسبوعياً على محتويات خادم الملفات.
- سيخصص مساحة منفصلة لحفظ الأرشيف.
- المساحة السحابية:

⇐ تم تزويد كل موظف وإدارة مساحة سحابية على OneDrive بحجم ١ تيرا بايت بإمكانه وضع الملفات التي يحتاج للوصول لها من خارج المكتب سواء من الجهاز المحمول أو الجوال أو أي متصفح، كما يمكن حفظ نسخ احتياطية من الملفات المهمة فيها.

ضبط الدخول للمعلومات والتطبيقات

- تقييد الدخول للمعلومات حسب الصلاحيات والأدوار عبر كل التطبيقات والأنظمة المستخدمة.
- يمنح المستخدمون صلاحية الوصول للمعلومات وفق متطلبات العمل فقط، ويتم تحديد الموافقات بناءً على دور الشخص في المؤسسة بما يرد من إدارة الموارد البشرية، ويتم تطبيق الضوابط التالية:
  - يمنح الدخول لخيارات كل تطبيق أو نظام وفق احتياجات المستخدم ودوره بالمؤسسة، كما هو موضح بتقسيم الأدوار والصلاحيات الموجود بالوثائق الخاصة بكل تطبيق.
  - ينتج عن التطبيقات والأنظمة مخرجات محددة وفق الأدوار المدرجة بالوثائق الخاصة بكل تطبيق أو نظام.
  - يمنح المستخدم الذي يحتاج الوصول لأي خدمة داخل المؤسسة وهو في خارجها (عن بعد) صلاحيات محدودة حسب حاجته وعبر آلية موثوقة وآمنة (VPN).

الحسابات والبريد الإلكتروني

البريد الإلكتروني:

- يحق لجميع المستفيدين الحصول على بريد إلكتروني خاص بهم تابع لنطاق شبكة المؤسسة يسمح له بإرسال واستقبال الرسائل الإلكترونية الخاصة بالعمل فقط.
- تقدم المؤسسة لأعضائها موارد وخدمات البريد الإلكتروني لمساعدتهم في أداء عملهم.
- يعد البريد الإلكتروني وسيلة رسمية للتواصل فيما يخص عمل المؤسسة.
- يجب أن تتوافق كافة أنواع التواصل التي يرسلها أعضاء المؤسسة من خلال نظام البريد الإلكتروني مع جميع سياسات المؤسسة، ولا يجوز الإفصاح عن أية معلومات سرية تعود ملكيتها للمؤسسة.
- المستخدم على علم ودراية أنه المسؤول الوحيد عما تحتويه الرسائل المرسلة من خلال حساب بريده الإلكتروني.
- يخضع استخدام البريد الإلكتروني للمؤسسة للمراقبة الدورية وسوء الاستخدام يعرضه للمساءلة.
- حساب البريد الإلكتروني الذي يتم تزويده للمستخدم من قبل المؤسسة يتم استخدامه لأغراض العمل الرسمي فقط، ولأغراض تبادل رسائل العمل والتعميمات المختلفة والملفات، ولا يجب استخدامه لأغراض شخصية أبداً أو غير قانونية أو غير مشروعة.
- البريد الالكتروني الخاص بالمستخدم ذو مساحة كبيرة لكن تظل محدودة، مما يترتب عليه وجوب قيام المستخدم دورياً بترتيب البريد وحذف غير المهم.
- يمنع نشر وإرسال رسائل غير متعلقة بالعمل الى مستخدمي البريد الإلكتروني الخاص بالمؤسسة وخصوصا استخدام مجموعة موظفي المؤسسة **Mail all ASF**.
- يجب على المستخدمين استخدام خدمات البريد الإلكتروني الرسمي للمؤسسة في المعاملات الرسمية، وعدم استخدام خدمات البريد الإلكتروني المجاني مثل **Hotmail**و**Yahoo** و **Gmail** .

- لا يسمح للمستخدمين بإرسال أو الرد أو توجيه رسائل البريد الإلكتروني ذو المحتوى السري أو التي تنتهك الحقوق.
- يحظر على المستخدمين ادخال أي تغييرات على المحتوى أو التاريخ أو الوقت أو المصدر أو الأشخاص أو العناوين أو أي معلومات أخرى في الرسالة الالكترونية.
- على المستخدمين استخدام التواقيع في المؤسسة مع كافة رسائل البريد الإلكتروني.
- يتم إدراج إخلاء المسؤولية تلقائيا لكل بريد يصدر عن إحدى حسابات المؤسسة.
- على المستخدمين عدم تسجيل عنوان البريد الإلكتروني الخاص بالمؤسسة في المواقع الالكترونية لغير أغراض العمل.
- على المستخدمين عدم فتح رسائل البريد الإلكتروني غير المرغوب فيها، مع حذفها من النظام.
- يحظر على المستخدمين استخدام البريد الإلكتروني للمؤسسة في المعاملات الخاصة.
- يحظر على المستخدمين المشاركة في نشر رسائل البريد الإلكتروني لأغراض خيرية دون موافقة مسبقة من جهة الاختصاص.
- يجب تذييل جميع البريد الإلكتروني الصادر من المؤسسة بفقرة إخلاء المسؤولية.

الحسابات:

- التعريف بالمستخدمين "الحسابات":
  - إنشاء الحسابات وحذفها يتم عن طريق إدارة التقنية بناء على دور الموظف في المؤسسة بإخطار من إدارة الموارد البشرية.
  - تعديل اسم مستخدم وصلاحيات الموظف يتم عن طريق تقديم طلب لمدير الإدارة التي يعمل بها الموظف وموافقة إدارة الموارد البشرية ويتم واعتماد الطلب من مدير إدارة التقنية وتنفيذه من خلال فريق إدارة التقنية.
  - يجب أن تخطر إدارة التقنية في حال حدوث تغييرات أو تنقلات في الموظفين التي قد تؤثر على أمن المعلومات، ومثالاً على ذلك الموظف الذي لديه حق الوصول إلى المعلومات السرية وينتقل إلى دور آخر حيث لا يشترط له هذا الوصول للمعلومات.
  - تقوم إدارة تقنية المعلومات بتزويد كل مستخدم بحساب خاص به مكون من اسم مستخدم (**User Name**) وكلمة سر (**Password**)، حيث قد لا يستطيع المستخدم الاستفادة من بعض خدمات شبكة المؤسسة إلا من خلال هذا الحساب الخاص به.
  - المستخدم مسؤول عن الحفاظ على سرية معلومات حسابه، والقيام بتغيير كلمة المرور دورياً، وأية عواقب تترتب على تسريب معلومات الحساب إلى مستخدمين آخرين يتحملها صاحب الحساب ولا تتحمل الإدارة أية مسؤولية.

- إنشاء وحذف الحسابات:
  - يتم إنشاء وحذف الحسابات اللازمة للموظف بناء على دوره في المؤسسة الصادر من إدارة الموارد البشرية.
  - خطوات حذف بريد عندما يتم الإبلاغ بالمغادرة النهائية لأي من منسوبي المؤسسة من قبل إدارة الموارد البشرية، تقوم إدارة التقنية المعلومات بتنفيذ مجموعة من الإجراءات وتتلخص فيما يلي:
    - ⇐ التأكيد على الموظف بنقل جميع بياناته الشخصية (بريد - ملفات).
    - ⇐ التأكيد على إدارة الموظف بنقل جميع البيانات الخاصة بالإدارة.
    - ⇐ يُحذف الحساب وصندوق البريد الإلكتروني وجميع الحسابات الخاصة بالموظف على أنظمة المؤسسة.
    - ⇐ يُحذف حساب المجال الخاص بالموظف.
    - ⇐ التأكد من إلغاء وحذف كافة حسابات الموظف السابق وتغيير بيانات الهاتف وإزالة الموظف السابق من كافة مجموعات مشاركة الملفات في خادم الملفات مع تأكيد على تغيير الرقم السري لبريد الإدارة.
    - ⇐ مراجعة كشف استلام الاحتياجات التقنية التي تسلمها الموظف طوال خدمته في المؤسسة ومطابقتها واستلامهما.

النسخ الاحتياطية واستعادة وحفظ البيانات

- تلتزم إدارة التقنية بإجراء النسخ الاحتياطي لجميع البيانات والمعلومات الموجودة على الشبكة من بيانات الأنظمة والمستخدمين والبريد الإلكتروني والمجلدات المشتركة بشكل دوري يضمن توفرها في حالة الحاجة.
- مسؤول الأنظمة هو المنوط بوضع خطط النسخ الاحتياطية كل حسب حاجة النظام على ألا تقل متطلبات تلك الخطط عن الحد الأدنى المنصوص عليه في السياسة، كما أن مسؤول الدعم الفني هو المنوط على أخذ النسخة الشاملة يومياً واسبوعياً وشهرياً وخارج الشبكة.
- كما أن المسؤول عن استرجاع النسخة الاحتياطية غير الشخص المسؤول عن عمل نسخة احتياطية.
- متطلبات الحد الأدنى للنسخ الاحتياطية:
  - تشمل خطط النسخ الاحتياطية بيانات المؤسسة، الأنظمة الداخلية بالمؤسسة، وجميع الخوادم، على أن يكون نواتج عملية النسخ قابلة للاسترداد.
  - يمكن استخدام صورة من صور النسخ الاحتياطية المعروفة مثل النسخ الكاملة (**Full Backup**)، النسخ التفاضلي (**Differential Backup**)، والنسخ التزايدي (**Incremental Backup**).
  - يجب ألا يقل مرات تكرار عملية النسخ الاحتياطية عن مرة يومياً للأنظمة وقواعد البيانات وأنظمة التشغيل الحساسة التي تحدث بياناتها يومياً.
  - يجب ألا يقل مرات تكرار عملية النسخ الاحتياطية عن مرة اسبوعياً لأنظمة التشغيل الخاصة بالخوادم.
  - يجب أن يتم اختبار عملية استعادة النسخ الاحتياطية دورياً للتأكد من فعالية عملية النسخ.
  - يجب تحديد عدد مدة حفظ النسخ الاحتياطية حسب أهمية المعلومات والبيانات على ألا تقل مدة حفظ النسخ عن ٩٠ يوم.
  - يجب الاحتفاظ بثلاث (٣) نسخ من ناتج عملية النسخ الاحتياطية في ثلاث (٣) أمكان مختلفة على الأقل.
  - يجب الاحتفاظ بنسخة احتياطية كاملة لمعلومات وبيانات المؤسسة في بيئة آمنة وخارج المؤسسة.
  - يتم عمل نسخ احتياطية من بيانات المؤسسة الموجودة على خادم مشاركة الملفات، والإدارة غير مسؤولة عن البيانات الهامة الموجودة على أجهزة الموظفين.
- يتم حفظ النسخ الاحتياطية في قرص تخزين بيانات خارجي شهرياً بالإضافة إلى النسخ المحلية.
- يتم رفع نسخة احتياطية من أنظمة تشغيل الخوادم أسبوعياً في مساحة التخزين السحابية.
- يتم رفع نسخة احتياطية من قواعد البيانات يومياً في مساحة التخزين السحابية.
- على المستخدم التأكد من نقل جميع الملفات الهامة والتي تتعلق بالعمل من سطح المكتب والمستندات إلى خادم الملفات في مجلد الإدارة ليسهل الوصول له من فريق الإدارة ولأنه يؤخذ له نسخة احتياطية دورية، وفي حال وجود ملفات لا ترغب بوضعها في خادم الملفات يفضل وضعها في مكان تخزين (قرص (D بعيدا عن مكان عمل نظام التشغيل وربطه في مساحة التخزين السحابية.
- تقوم إدارة التقنية بتوفير أعلى مستويات الأمن الإليكتروني والحماية للبيانات التابعة للشركة من خلال استخدام الأجهزة والبرامج المساندة لذلك مثل برامج مضادات الفيروسات وبرامج مكافحة الاختراق وتقنيات الجدار الناري.

الدعم الفني

تقوم الإدارة بأعمال الصيانة بأنواعها المختلفة لأجهزة ومعدات تقنية المعلومات بالمؤسسة وتقوم أيضاً بتوفير الدعم الفني لجميع منسوبي المؤسسة، ويتمثل هذا الدعم بتقديم المساعدة وتوفير الحلول على مستوى البرامج وأجهزة تقنية المعلومات من خلال فريق متخصص في هذا المجال. وتتمثل أهداف الإدارة في الآتي:

- تنفيذ أعمال صيانة أجهزة والطابعات بالمؤسسة والمهام الأخرى المناطة بالإدارة بأقصى درجات الكفاءة والجودة وبأقل التكاليف الممكنة.

- المحافظة التامة على البنية التحتية لتقنية المعلومات بالمؤسسة وما تحتويه من معدات وذلك من خلال إجراء الصيانة الوقائية والتصحيحية الفعالة.
- الالتزام دائماً بالشروط والمواصفات والضوابط المحددة في الاتفاقيات المبرمة بين المؤسسة والشركات عند تنفيذ أعمال الصيانة بالمؤسسة بما يحفظ حقوق المؤسسة ويؤدي إلى أفضل النتائج.
- تقليل المدة اللازمة لإصلاح الأعطال التي تطرأ إلى أدنى حد ممكن وحل المواضيع والمشكلات التي تواجه الصيانة بالطرق الفعالة والمثلى.
- أن تحظى الخدمات المختلفة التي قدمها القسم على رضا منسوبي المؤسسة من حيث جودة هذه الخدمات والسرعة في تقديمها.
- أن يمتلك جميع تقنيو القسم المهارات والقدرات اللازمة لتأدية المهام المناطة بهم على أكمل وجه وذلك من خلال التدريب والتأهيل والاطلاع على الطرق الحديثة في أداء العمل.
- تطوير العمل والرقي به من خلال استخدام التقنية والطرق الحديثة في أدائه.
- حل جميع المشاكل التطبيقية والتشغيلية المتعلقة بتقنية المعلومات عن طريق توفير المساعدة والتوجيه لجميع موظفي المؤسسة.
- المساهمة في تحقيق أهداف المؤسسة المنشودة بالقيام بما يطلب من القسم في مجال اختصاصاته.
- يمنع منعاً باتاً القيام بمحاولة تغيير توصيلات شبكة الحاسوب في المؤسسة، كما يمنع القيام بمحاولة فتح صندوق أجهزة الحاسب كما يعلم المستخدم أن صلاحيات التوصيل والتغيير وفتح أجهزة الحاسوب وصيانتها تقتصر على قسم الدعم الفني.

الصيانة الدورية الوقائية

- تقوم إدارة التقنية بعمل صيانة دورية للحفاظ على الأجهزة والطابعات في حالة جيدة.
- يتم عمل الصيانة الدورية ٣ مرات على مستوي العام وفي شهور محددة.
- الدورية الأول في شهر ٢ ميلادي.
- والدورية الثانية في شهر ٧ ميلادي.
- والدورية الثلاثة في شهر ١٠ ميلادي.
- وفي كل دورة يتم التركيز على بعض النقاط.
- تختلف الأولوية على حسب أولوية الموظفين مثال:
  - كثرت المشاكل في جهاز إدارة معينة او جهاز معين.
  - حسب الأهمية: الادارات الخيرية ثم المالية والإدارية ثم القاعات.
  - حسب الإتاحية للموظف ووجوده.
- العدد الأجهزة التي يتم عمل صيانة لها في اليوم من ٢ إلى ٥ وتختلف حسب ضغط العمل.
- لكل دورة قائمة تفقد ثابتة ومصنفة يتم فحصها ومصنفه حسب الأهمية وتراجع دورياً، كما أنه قد يضاف لها بعض الخطوات في كل دورة.

الخطوات المتبعة لتطبيق الصيانة:

- تحديد الأجهزة المراد صيانتها.
- تحديد ما سوف يتم في الصيانة.
- عمل الجداول الخاصة بعمليات الصيانة.
- استحداث خطة الصيانة.
- توفير قطع الغيار.
- تسجيل المعلومات في كل دورة صيانة.

- إدارة التقنية هو المسؤول عن استقبال جميع المشكل المتعلقة بالخدمات التقنية.

- يوفر قسم تقنية المعلومات الرقاب والمتابعة والصيانة الدورية اللازمة للخادم، الأجهزة وملحقاتها، الشبكات، خدمة الانترنت، الهاتف، البريد الالكتروني، وغيرها بما يضمن الاستمرارية والكفاءة في الأداء.
- على إدارة التقنية وضع جدول زمني خاص بصيانة الدورية لكل أجهزة الحاسب وملحقاته والشبكات تحديث الأجهزة والبرامج التابعة للشركة لتفادي حدوث المشاكل.

الاحلال والتجديد للبنية التقنية بالمؤسسة

يتيح عملية الإحلال والتجديد للبنية التحتية التقنية (الأجهزة المكتبية – السيرفرات - التليفونات) تلافي أي مشاكل تقنية بشكل كبير وتجنب توقف العمل بالمؤسسة.

- يتم عمل الاحلال والتجديد من خلال تحديد العمري الافتراضي لكل جهاز.
- يتم تحديد العمر الافتراضي من خلال إدارة الأصول في المالية والتي تحدد العمر الافتراضي لكل الأجهزة.
- وبعد تحديد العمر الافتراضي يتم قياس مدا كفاية الأجهزة ويتم إعادة تقيم للجهاز بشكل عام ثم يتخذ الإجراء الأنسب سواء باستبداله أو بتمديد فترة خدمته أو في نهاية عمر كل جهاز يتم تقييمية مره أخرى ويتم اتخاذ قرار باهلاكه أو تجديد العمل به لمدة محدده.
- يجب شراء الحواسيب المكتبية وفق المواصفات القياسية المحددة من قبل إدارة التقنية والخاصة بأجهزة الاستخدام للعمل وليس للاستخدام الشخصي).
- يقيم إدارة التقنية ويستشير المصنعين ووكلاء البيع المتخصصين لاختيار أفضل ما يناسب المؤسسة من حيث العلامات التجارية العالمية وجودة الطراز والسعر والكفاءة.
- يشرف إدارة التقنية على عملية شراء واستلام وتوزيع أجهزة الحواسيب المكتبية والمحمولة والأجهزة الطرفية بحسب الخطة الموضوعة من قبل إدارة التقنية وبناءً على صلاحيات الصرف المتوفرة.