لائحة تكنولوجيا المعلومات

إعداد اللائحة	إعتماد اللائحة
قطاعات الدعم (قطاع تكنولوجيا المعلومات)	

لائحة تكنولوجيا المعلومات

الأحكام العامة

مادة: (1)

تهدف هذه اللائحة إلى تحديد القواعد والإجراءات التى تنظم إستخدام الأنظمة الإلكترونية بشكل عام و تشمل هذه الأنظمة (أنظمة SAP ، وأنظمة ميكنة العمليات الإنتاجية، وميكنة أنظمة الصيانة، وميكنة أنظمة الموازين، والبريد الإلكترونى، والإنترنت، وأنظمة التخزين الإلكترونى للملفات، والمستندات ، الخ) بشركة بورسعيد الوطنية للصلب، أوشركة آى آى سي، لإدارة مصانع الصلب، أو شركة حديد المصريين لتجارة مواد البناء أو شركة حديد المصريين لإدارة مشروعات مصانع الصلب أو المركز الرئيسي بهدف ضمان صحة ودقة وأمن البيانات والمعلومات المتاحة على هذه الأنظمة وسلامة طرق تداولها وحفظها وتشغيلها وإسترجاعها لمستخدميها فى الشركة.

مادة: (2)

السلطة المختصة ويرد نطاق إختصاصاتها بمصفوفة الصلاحيات الرسمية للشركة والتى يحددها مجلس الإدارة والتى تصدر و تعدل بقرارمنه.

فى حالة غياب المختص بالإعتماد يحل محله من هو مكلف بالقيام بعمله فى فترة غيابه بعد الموافقة المسبقة من الرئيس المباشر, وبالنسبة لرؤساء القطاعات فيتوجب الموافقة المسبقة من العضو المنتدب.

مادة: (3)

أحكام هذه اللائحة ملزمة لجميع الموظفين بالشركة ومن يخالف أحكامها يتعرض للمساءلة القانونية طبقاً للائحة الجزاءات المعمول بها بالشركة ، وإذا كانت المخالفة تشكل جريمة جنائية فيتم إتخاذ الإجراءات القانونية حيالها.

تراجع بنود هذه اللائحة كلما دعت الضرورة لذلك للتأكد من تلبيتها لإحتياجات الشركة

ترسل هذه اللائحة للعاملين عن طريق البريد الإلكتروني للشركة بشكل دورى (على الأقل مرة واحدة سنوياً) وذلك لإعلام وتذكير الموظفين القدامى والجدد بها.

مادة: (4)

تعتمد هذه اللائحة من قبل مجلس إدارة الشركة ولا يجوز تعديل أو تغيير أى مادة أو فقرة فيها إلا بموجب قرار صادر عنه، وفى حالة صدور أى تعديلات ينبغى تعميمها على كل من يهمه الأمر قبل بدء سريانها بأسبوع على الأقل ، و يعمل بأحكام هذه اللائحة إعتباراً من اليوم التالى لموافقة مجلس الإدارة عليها.

تسرى على العمليات و/أو الإجراءات بالنسبة للغير التى تم البدء فيها قبل تاريخ سريان هذه اللائحة أحكام الإتفاقات التى أبرمت على أساسها حتى نهايتها أو بتعديلها وفق أحكام هذه اللائحة ما أمكن.

لائحة تكنولوجيا المعلومات

أولاً: إستخدام تكنولوجيا المعلومات

مادة: (5):

إنشاء حسابات للمستخدمين الجدد، و تعديلها، و إلغاؤها على شبكة معلومات الشركة، و نطاقاتها، و برنامج ال SAP

يتم إنشاء حسابات للمستخدمين (الموظفين) الجدد مع الصلاحيات المناسبة و المطلوبة لهم بناءً علي طلب رسمي من إدارة الموارد البشرية، و ذلك بعد اعتمادها في الموازنة العامة، و يحدد في هذا الطلب بيانات المستخدم كاملةً علي أن تتضمن اسم المستخدم بالكامل و الشركة المعين بها، و مركز التكلفة و طبيعة نشاط المستخدم و مدي احتياجه لكمبيوتر محمول أو مكتبي و تاريخ التحاقه بالعمل.

و في حالة الاحتياج لإنشاء حساب و تقديم أجهزة حاسب لمستخدم غير مشمول في الموازنة لابد من الحصول علي الموافقات الإدارية المطلوبة خارج الموازنة طبقاً لسياسة الشركة,

كما يقدم طلب منفصل في حالة احتياج المستخدم لإنشاء حساب علي برنامج ال SAP، طبقاً للمادة رقم 10

في حالة انتهاء عمل الموظف، يتم وقف جميع حسابات المستخدم فورياً علي كل النظم، و تترك لمدة ثلاثون يوماً لدراسة مدي احتياج إدارته لأي معلومات مسجلة لهذا المستخدم، علي أن يتم حذف الحساب نهائياً بعد ذلك.

و يتم تفعيل هذا الإجراء مع وصول إخطار رسمي من قطاع الموارد البشرية أو المدير المباشر أو وصول إخلاء الطرف للموظف لقطاع نظم المعلومات.

أصول ومعدات وأدوات الحاسب الآلى

يمسك قطاع الحاسب الآلى سجلاً يتضمن قاعدة بيانات لتتبع ورقابة أصول الحاسب الآلى التى صرفت من المخازن الرئيسية وأصبحت فى عهدة الموظفين أو الإدارات المختلفة لخفض مخاطر فقد المعلومات والبيانات أو الاصول ذاتها المملوكة للشركة .

يلتزم قطاع المخازن بتسجيل الإضافات والمنصرف والمرتجع من أصول ومستهلكات الحاسب الآلى (طبقاً لإجراءات المخازن الواردة بلائحتى المشتريات والمخازن) على أن يتم التمييز بين طرق التسجيل كالآتى:

- **الأصول الثابتة وتتضمن البنود الآتية:**

1. أجهزة الحاسب المكتبية
2. أجهزة الكمبيوتر المحمول "لاب توب "

3. الطابعات وآلات تصوير المستندات وآلات الفاكس وآلات متعددة الوظائف
4. الأجهزة الحاسب المحمولة"
5. الماسحات الضوئية
6. دوك ستيشن
7. الخادم / سيرفر
8. الموجهات و المحولات
9. الشاشات وأجهزة عرض
10. التليفونات المكتبية
11. كاميرات المراقبة
12. أجهزة توجيه بيانات لاسلكية
13. وسائط تخزين البيانات

يقدم الموظف أو الإدارة طلباً لقطاع تكنولوجيا المعلومات بإحتياجاته معتمداً من رئيس القطاع ويحدد به الأصناف المطلوبة سواء للموظف أو للإدارة.

ويقوم تبعاً لذلك قطاع تكنولوجيا المعلومات بتحويل ذلك الطلب إلى طلب صرف من المخازن في حالة توافر الأصل أو الأصول المطلوبة، و تجدر الإشارة بأنه لا يمكن لأى إدارة تقديم طلبات صرف لأصول ثابتة - للحاسب الآلى مباشرة إلى قطاع المخازن.

يتولى قطاع تكنولوجيا المعلومات بالمركز الرئيسي القيام بأعمال مخازن مستلزمات تكنولوجيا المعلومات من الإضافة والتخزين والصرف.

ويقوم قطاع المخازن بكل مصنع بصرف الأصناف المطلوبة إلى قطاع تكنولوجيا المعلومات فعلياً الذى يقوم بدوره بتسليم الأصناف إلى الموظف أو الإدارة الطالبة ويوقع على إقرار إستلام العهدة.

(فى حالة ما إذا كانت الطلبات تخص موظفاً جديداً, يقوم قطاع الموارد البشرية بتحرير طلب بالأصناف بدلاً من القطاع)

ويوجه بعد ذلك قطاع تكنولوجيا المعلومات صورة من مستند الصرف مصحوبة بصورة من إقرار إستلام الموظف/الإدارة لقطاع الرقابة المالية من اجل تسجيل عهدة الأصول الثابتة على الموظف أو الإدارة بسجل الأصول الثابتة على SAP.

- **المستهلكات وتشمل البنود الآتية:**

1. أحبار للطابعات
2. شنط لأجهزة الكمبيوتر المحمولة

3. لوحة مفاتيح و فأرة
4. بطاقات الفيديو وبطاقات الصوت
5. كابلات توصيل بيانات و فيديو و **USB**، و خلافه
6. أقراص التخزين الصلبة الخارجية ، و أقراص التخزين المؤقتة (فلاشات)، الخ.

يقدم الموظف أو الإدارة طلباً لقطاع تكنولوجيا المعلومات بإحتياجاته معتمداً من الرئيس المباشر للموظف ويحدد به المستهلكات المطلوبة للإدارة.

ويقوم تبعاً لذلك قطاع تكنولوجيا المعلومات بتحويل ذلك الطلب إلى طلب صرف من المخازن (لا يمكن لأى إدارة تقديم طلبات صرف مستهلكات حاسب آلى مباشرة إلى قطاع المخازن)

ويقوم قطاع المخازن بكل مصنع والمركز الرئيسي بصرف المستهلكات وتحميل التكلفة على مركز تكلفة الإدارة الطالبة.

مادة: (6)

ضوابط التخزين الإلكتروني للملفات على أجهزة الحاسب الآلى المخصصة لمستخدمى الشركة و الحاسب الخدمى (سيرفر الشركة)

توفر الشركة على السيرفر العام مساحة تخزين محدودة ومؤمنة لكل مستخدم مصرح له بالدخول على الشبكه وبذا يمكن للعاملين المصرح لهم بالوصول للملفات الموجودة على السيرفر مما يعد وسيلة لحماية البيانات من الضياع، ويتم تحديد مساحة التخزين لكل موظف وفقا لموارد الشركة ومسؤلياته الوظيفية.

ويتحتم وجود حساب مستخدم فعال للدخول علي شبكة الشركة ويرمز لقرص التخزين الافتراضي على كل جهاز لأى موظف بالحرف **"H"**

ويلتزم الموظفين بحفظ ملفاتهم الإلكترونية المتعلقة بالعمل على قرص التخزين الإفتراضى المشار إليه وتعد مخالفة ذلك مسئولية يحاسب عليها الموظف طبقاً للوائح الشركة (الملفات المتعلقة بالعمل هى كل ما هو متعلق بالعمل وينتج عن فقده آثار سلبية على العمل والشركة)

ويتوجب على جميع الموظفين الإلتزام بالإجراءات التالية :

1- يقوم قطاع تكنولوجيا المعلومات بعمل نسخة احتياطية من السيرفر العام والذى يتضمن قرص التخزين **H** المشار إليه لكل موظف.
2- الملفات الأخرى الموجودة على القرص الصلب الخاص بجهاز الحاسب الشخصي للمستخدمين والغير مرتبطة بالعمل غيرتلك المخزنة على القرص الإفتراضى **H** تعد مسئولية الموظف ولا مسئولية على الشركة فى حال فقدها.
3- لا يسمح بتخزين ملفات الصوت أو الفيديو أو غيرها من الملفات الشخصية غير المرتبطة بالعمل على أجهزة الشركة والسيرفر العام.
4- في حالات خاصة وعند تقديم أسباب واضحة تتعلق بالعمل وتعتمد من رئيس قطاع تكنولوجيا المعلومات، تمنح استثناءات للبند رقم 3 وتكون الاستثناءات لعدد محدود من المستخدمين أو الإدارات مثل قطاع الإتصالات والعلاقات العامة وإدارة التسويق.
5- في حالة الحاجة لاستعادة ملفات معينة، يكون هذا وفقا للنسخ الاحتياطية وسياسة الاستعادة ودورة الحفظ المطبقة من قطاع تكنولوجيا المعلومات علما بأن اقصي مده يمكن من خلالها استعادة البيانات المخزنه هي 90 يوما او حسب الإمكانيات التخزينيه للشركه المتاحه في كل موقع من مواقع الشركه على حده.

مادة: (7)

ضوابط إستخدام البريد الإلكترونى

يعد إستخدام البريد الألكترونى للشركة من وسائل الإتصال المعتمدة بها ويتطلب إستخدامها الإلتزام الكامل بالإجراءات التالية بما يحقق الإستخدام الملائم لجميع حسابات البريد الإلكترونى:

1- عند التواصل باستخدام نظام البريد الإلكتروني الرسمي، يجب مراعاة أعلى المعايير الاحترافية حيث أن هذه الرسائل البريدية تمثل الشركة عند إرسال بريد رسمي أو عند الرد علي بريد رسمي.
2- لا يتم استخدام بريد إلكتروني شخصي من الموظفين بالشركة عند إرسال المراسلات الرسمية مع الموردين او العملاء او مقدمي الخدمات أو البنوك أو الجهات الرسمية أو أى أطراف أخرى تتعامل أو فى سبيلها للتعامل مع الشركة، ويستخدم البريد الإلكتروني الرسمي فقط للقيام بأي مراسلات رسمية عبر البريد الالكتروني.
3- فى حال وصول بريد إلكترونى من أحد المتعاملين مع الشركة إلى البريد الرسمي للشركة فيحظر على الموظفين إعادة توجيه مثل هذه المراسلات إلى عناوين البريد الإلكترونى الشخصية للموظفين أو أى طرف ثالث غير معنى بهذه الرسائل.
4- كما يجب على الموظفين توخي الحذر الشديد عند فتح رسائل البريد الإلكتروني وخاصة المرفقات الواردة من مرسلين غير معروفين، والتي قد تحتوي على فيروسات وديدان إلكترونية أو علي اكواد لفيروسات حصان طروادة.
5- لا ينبغي أن يزيد حجم مرفقات البريد الألكترونى عن ٥٠ ميجابايت في كل بريد إلكتروني مرسل داخل الشركة، مع تفضيل تقليل حجم الملفات كلما أمكن، و تجدر الإشارة أن حجم الملفات المرسلة للجهات الخارجية يعتمد علي نظام البريد الالكتروني للجهة المستقبلة و التي قد تسمح بحجم أقل من الرقم السابق المشار إليه.
6- وفى حالة الحاجة لإرسال مراسلات تحتوى على مرفقات تزيد عن القيمة المشار إليها فيتوجب على المرسل تجزئة المرفقات على أكثر من بريد إلكترونى أو الرجوع لقطاع تكنولوجيا المعلومات لتوفير البديل المناسب.
7- ويحظر إرسال رسائل البريد الإلكتروني نيابة عن مستخدمين آخرين دون الحصول على موافقة مسبقة وتفويض من ذلك المستخدم.

8- كما يحظر إرسال أي بريد إلكتروني من قبل الموظفون من البريد الإلكتروني الرسمي الخاص بالمجموعة إلى وسائل الإعلام المختلفة دون الحصول على موافقة مسبقة من رئيس مجلس الإدارة والعضو المنتدب إلا فى حالة صدور تفويض أو تكليف لجهة ما بالشركة بذلك

9- يجب استخدام توقيع البريد الإلكتروني الرسمي والتذييل بإخلاء المسؤولية الموزعة من قبل الشركة دون اي تعديل عليهما سوي باضافة المعلومات الشخصية.

10-فى حالة الإرتياب فى وصول بريد إلكترونى قد يحتوى على فيروسات أو ما قد يضر أنظمتها الألكترونية فيحظر إعادة ارسال مثل هذه الرسائل داخل الشركة ويتوجب الإتصال المباشر بقطاع تكنولوجيا المعلومات عن طريق الهاتف.

11-لا يجوز استخدام نظام البريد الإلكتروني الرسمى للشركة لإنشاء أو توزيع أي رسائل تخريبية أو هجومية، بما في ذلك التعليقات المسيئة التي تتناول العرق أو النوع الاجتماعى أو اللون أو الإعاقة أو العمر أو التوجه الجنسي أو المواد الإباحية أو المعتقدات الدينية أو الشعائر الدينية أو المعتقدات السياسية أو الأصول القومية ويعرض الموظف الذى يقوم بذلك للمساءلة القانونية والعقوبات طبقاً للوائح الشركة والقوانين الخاصة بذلك، ويتوجب على الموظفين ممن يتلقون أي رسائل على البريد الإلكتروني تتضمن المحتوى سابق الذكر من أي موظف داخل الشركة أو من خارجها، إبلاغ المدير المباشر والرئيس التنفيذى لقطاعات الدعم والإدارة القانونية فورا.

ولقطاع تكنولوجيا المعلومات إتخاذ الإجراءات الفورية بإيقاف اي حساب بريد الكتروني مخالف لما سبق من معايير أو مخالفة آية معايير أخرى يراها القطاع لم تكن واردة بعاليه وتؤثر سلباً على حماية أنظمة الشركة الألكترونية مع عرض الأمر على الرئيس التنفيذى لقطاعات الدعم.

كما يجوز لقطاع تكنولوجيا المعلومات إيقاف أى بريد إلكترونى غير مستخدم لأكثر من 30 يوماً؛ وذلك لاعتبارات الأمن والتدقيق، بعد التحقق من قطاع الموارد البشرية عن مثل هذه الحالات قبل اتخاذ الاجراء سابق الذكر، ويجوز لقطاع تكنولوجيا المعلومات حذف اي حساب بريد الكتروني غير مستخدم بعد مضي 90 يوم؛ وذلك بعد التنسيق مع إدارة الموارد البشرية والحصول على تاكيد منها للقيام بذلك.

مادة: (8)

ضوابط تسجيل الدخول على شبكة الإنترنت واستخدامها

حيث أن الشـــركة تهدف من توفيرها لخدمة الإنترنت إلى تمكين الموظفين من إســـتخدامها للقيام بمهامهم الرسمية وتيسيرها عليهم سواء كان هذا الإستخدام عبر أجهزة الحاسب الآلى المخصصة لهم أو الأجهزة التي يمكنها الدخول إلي الإنترنت أو كليهما مع العلم بأن الإستخدام غير المصرح به للإنترنت قد ينتج عنه إلحاق الضـرر بالأنظمة الآلكترونية للشـركة وفقدان البيانات أو قد يعرض الشـركة لمخالفة القوانين ولذا فإنه يتوجب على الموظفين الإلتزام بالإجراءات الآتية عند إستخدامهم لهذه الخدمة:

1- يسمح لموظفي الشركة استخدام الإنترنت لأسباب تتعلق بالعمل.
2- يحظرتحميل المواد التي تخضع للحماية وحقوق التاليف والنشر من الإنترنت.
3- يحظر اســـتخدام حســـابات تخزين على الانترنت مثل: "yahoo briefcase أو google drive" لتخزين وثائق أو ملفات أو ابتكارات مملوكة للشركة.
4- يحظر استخدام برامج (سيرفر بروكسي) بدلا من تلك المصرح بها من الشركة، أو أن يقوم أحد الموظفين من الشركة أو من أطراف خارجية بمحاولة تجاوز أو إتباع أي أسلوب مناورة لتجاوز برامج الحمايه الموجوده بالشركه.
5- يحظر بشـكل قاطع محاولات اجراء مسـح للبورتات أو المسـح الأمني على اي من سـيرفرات الشركه.
6- يمنع تنفيذ أي شكل من أشكال مراقبة الشبكة لاعتراض أي بيانات غير مرسله للموظف بصوره طبيعيه.
7- لا يسمح باستخدام أي معدات إنترنت لاسلكي أخرى (واي فاي) من أجل تجاوز خدمة الإنترنت المراقبة والمحمية داخل الشـركة في مقرها أو بالقرب منها، دون الحصـول على إذن مسـبق من رئيس قطاع تكنولوجيا المعلومات الذى قد يصرح بذلك في حالة الضرورة لاستكمال العمل حال إنقطاع الخدمة.
8- يمنع منعا باتا تحميل أي برامج من الإنترنت أو الأقراص و الوسـائط الخارجية دون إذن مسـبق من قطاع تكنولوجيا المعلومات، بســبب المخاطر والتهديدات المحتملة المرتبطة بها، بالإضـــافة إلي حقوق الملكية الفكرية وبالتالي فإن قطاع تكنولوجيا المعلومات ســـيتخذ جميع الإجراءات اللازمة لمنع أي تحميل غير مصرح به للملفات القابلة للتنفيذ.

9- يجب ألا يستخدم الدخول على الإنترنت في أي نشاط غير قانوني أو للوصول إلى مواد غير قانونية أو الوصول إلى المواد التي تشتمل علي الفئات التالية، علي سبيل المثال لا الحصر:

10-المحتويات المخصصه للبالغين أو الناضجين أو التعارف أو العلاقات الشخصية أو الكحول أو الإنتحال أوالمواد الإباحية أو الروحانيات أو المخدرات أو الغيبيات أو القمار أو أدوات الدخول عن بعد أو الألعاب أوالأعمال الفنية أو التعليم الجنسي أو الإختراق أو صفحات الفكاهة أو النكات أو تحميل البرامج الغير مصرح بها أو برامج إبطال البروكسى أو مصادر البرمجيات الخبيثة أو الاستبيانات غير القانونية أو برامج بث الصوت والفيديوأو الصفحات العسكرية أو تلك التى تحرض على العنف أو الكراهية أوالإرهاب.

قد يتم مراقبة جميع أنشطة المستخدمين علي الإنترنت من خلال قطاع تكنولوجيا المعلومات أليا عن طريق اجهزة الحمايه داخل الشركه وفي حالة ملاحظة آياً مما أشير إليه من قواعد أو تعاملات مشكوك فيها على شبكة الشركة، فيقوم قطاع تكنولوجيا المعلومات بإتخاذ جميع الإجراءات اللازمة لرصد وكشف ومنع أي إنتهاك.

ويقدم رئيس قطاع تكنولوجيا المعلومات تقارير دورية للرئيس التنفيذى لقطاعات الدعم بالمخالفات التى يتم رصدها لهذه الإجراءات والتى يعد انتهاكها مخالفة قد تؤدى إلى اتخاذ إجراءات تأديبية أو قانونية أو كليهما كما قد تصل لإنهاء الخدمة حال تكرار المخالفة بعد موافقة السيد رئيس مجلس الإدارة والسيد العضو المنتدب.

مادة: (9)

في حالة وجود سبب واضح متعلق بالعمل، يجوز لبعض الموظفين ممن تتوفر لديهم الحاجة للدخول الى إحدى المحتويات المغلقة على الإنترنت ملء "إستمارة منح حق دخول" وذلك بعد الحصول على موافقة رئيس القطاع للموظف المعني، يتم تحويل الطلب الى قطاع تكنولوجيا المعلومات لمنح الموظف إمكانية الدخول الى المحتوى المطلوب مع تقديم سبب واضح متعلق بحاجة العمل وتحديد المواقع المراد الدخول عليها استثنائيا وتحديد مدة تصريح الدخول.

ثانياً: برامج تطبيقات الأعمال

مادة: (10)

برامج تطبيقات الأعمال وصلاحيات الدخول عليها

تعتمد الشـــركة فى دورات العمل المختلفة على عدد من البرامج الإلكترونية (على ســـبيل المثال برنامج **SAP**) والتى تنفذ من خلالها القطاعات المختلفة إجراءات أعمالها كالبيع والشـــراء والمخازن والمالية والموارد البشـــرية ، الخ. ولتنظيم الدخول على هذه البرامج واســـتخداماتها المختلفة وإجراءات تحديثها والتغيرات التى قد تتطلبها دورات العمل المختلفة على هذه البرامج لضـبط نقاط الرقابة عليها أو لتواكب دورات العمل الفعلية، فإن قطاع تكنولوجيا المعلومات قد حدد الإجراءات التالية للإلتزام بها من جميع مستخدمى هذه البرامج :

1- إن دخول الموظفين على البرامج الخاصـــة بالعمل (**SAP**) هو إحدى حاجات العمل، وبالتالي فإن طلب الموظفين منح حق الدخول على هذا البرنامج وتحديد الصـــلاحيات المطلوبة أو طلب صـلاحيات أوسـع من الصـلاحيات الحالية سـواء للمستخدمين الحاليين أو الجدد، فإن ذلك يكون من خلال تقديم طلب مكتوب أومن خلال بريداً إلكترونياً يعده الموظف ويحدد بـه إحتياجاتـه ويعتمد مديره المباشـــر ورئيس القطاع المعنى (بالإضـــافة إلى رئيس القطاع المختص بالجزء المطلوب الدخول عليه من القطاعات الأخرى وذلك في حالة وجود أكثر من إدارة معنية بهذه البيانات) قبل منح حق الدخول على برنامج الأعمال.
2- يتم إنشاء حسابات المستخدمين التي تمكنهم من الدخول بكلمة سر بقيمة مبدئية موحدة، وتستخدم للدخول لمرة واحدة فقط ويجبر المســتخدم على تغيير كلمة المرور وفقا لســياســة كلمة المرور المطبقة والإجراءات.
3- يلتزم مســـتخدمى التقارير بإظهار أعلى معايير النزاهة والســـلوك الأخلاقي من خلال الالتزام بســرية التقارير التي تغطي الجوانب المالية وغير المالية للشــركة، مع تعرض من يخالف ذلك للمسائلة طبقاً للوائح الشركة والقوانين السارية.

4- يلغى دخول المستخدم على هذه البرامج سواء عند انتهاء عمله مع الشركة، أو في حالة نقل موظف إلى وظيفة أخرى داخل الشركة لا تتطلب مسئولياتهم الجديدة الصلاحيات الحالية الممنوحة على هذه البرامج ، أو بناء على إخطار رسمي من رئيس القطاع الذى يعمل به الموظف بتعديل الصلاحيات الممنوحة له.

5- يرسل قطاع تكنولوجيا المعلومات بطلبات إضافة أو تعديل الصلاحيات من القطاعات المختلفة إلى قطاع المراجعة الداخلية لإبداء الرأى فيما تطلبه القطاعات من صلاحيات وما قد يؤديه منحه أو توسيع أو تقليص الصلاحيات من تعارض للمصالح أو فتح ثغرات فى النظام الرقابى لهذه البرامج.

6- يلتزم قطاع تكنولوجيا المعلومات علي أستمرار إتاحة العمل على برامج الأعمال دون تعطل قدر الإمكان وتقليص أوقات التعطل إلى الحد الأدنى طبقا لمعايير الصناعة.

7- فى حالة حاجة أحد القطاعات لإجراء تعديلات على برامج الأعمال المشار إليها، فتقوم الجهة/ الإدارة الطالبة للتعديلات بإعداد مستنداً (نموذج طلب التغيير) يوضح به التعديلات المقترحة وتناقش مع إدارة نظم المعلومات، و يتم البت في الطلب حسب الوارد في مادة رقم # ١٢.

مادة: (11)

التقارير التى تصدر من برامج الأعمال

توفر برامج الأعمال عدداً من التقارير التى تستخدم فى إتخاذ القرار على كافة المستويات، ويحدد قطاع تكنولوجيا المعلومات الإجراءات التالية لتنظيم الدخول على واستخدام هذه التقارير فضلاً عما قد تطلبه القطاعات المختلفة من تغييرات فى تصميمات هذه التقارير للوفاء بإحتياجاتهم :

1- يجب منح حق الدخول وإستخدام هذه التقارير طبقا لطبيعة أدوار الموظفين والحاجة لمعرفة المعلومة التى يوفرها التقرير مع الإلتزام بمبادئ فصل المهام ومنع تضارب المصالح

2- يعد دخول الموظفين على التقارير التي تنتجها التطبيقات إحدى احتياجات العمل، وبالتالي فإن تعليمات منح حق الدخول أو زيادة السلطات للمستخدمين الحاليين أو الجدد يطلبها الموظف ويعتمدها رئيس القطاع المعنى (بالإضافة إلى رئيس القطاع المختص بالجزء المطلوب الدخول عليه من القطاعات الأخرى وذلك في حالة وجود أكثر من إدارة معنية بهذه البيانات) قبل منح حق الدخول على التقارير وإستخدامها.

3- يلتزم مســـتخدمى التقارير بإظهار أعلى معايير النزاهة والســـلوك الأخلاقي من خلال الالتزام بســـرية التقارير التي تغطي الجوانب المالية وغير المالية للشـــركة، مع تعرض من يخالف ذلك للمسائلة طبقاً للوائح الشركة والقوانين السارية.

4- يجوز لمســـتخدمى التقارير من القطاعات المختلفة أن يطلبوا تعديلاً لتصـــميم بعض التقارير لعرض بعض البيانات بشـــكل مختلف بما يحقق اهداف القطاعات من خلال اســـتخدام هذه التقارير، ويعد القطاع نموذج طلب تعديل لتصـــميم التقرير معتمداً من رئيس القطاع الطالب (على أن يتضـــمن الطلب الجدول الزمني المطلوب لإعداد التغيرات المطلوبة وتفاصـــيل التعديلات ألخ.

5- يقوم قطاع تكنولوجيا المعلومات بترتيب أولويات إعداد التغيرات المطلوبة طبقاً لخطط عمل القطاع، وفور إعداد التقارير المطلوبة يتكم عرض النتائج على القطاع الطالب لإتمام إجراءات الإختبار اللازمة والقبول للنتائج أو رفضـــها من القطاع الطالب، ويتم ذكر الاســـباب التي بني عليها الرفض لمقدم الطلب في حالة رفض طلبه، ثم تؤخذ هذه الأســـباب فى الإعتبار عند إعادة تنفيذ التغيرات على التقارير.

6- يتم تطبيق التقرير المعتمد علي بيئة اختبار، وسيقوم المستخدمون باتباع خطة للإختبار للتأكد من أن المتطلبات مدخلات التقرير صـــحيحية وان النتائج جاءت وفق المتوقع، وفى هذه الحالة يوقع مســـتخدمى التقرير على نموذج طلب التعديلات بقبول النتائج تمهيداً لإســـتخدام التقريربشـــكل رسمى فى بيئة العمل الرسمية (مع توثيق جميع ما سبق من إجراءات).

7- يجب على كافة المســتخدمين عند إســتخدام التقارير وضــع نقاط التنقية أو التصــفية أثناء عملية انتاج التقارير والتأكد من أنهم ينتجون تقارير تغطي المعلومات المطلوبة فقط.

8- يجب على كافة المســتخدمين التأكد من عدم ازدواجية التقارير بحيث لا يتم اســتهلاك حجم كبير من موارد النظام وان يتم تطوير تلك التقارير في مواعيد دورية يتم الاتفاق عليها.

9- يلغى دخول المســتخدم على هذه التقارير ســواء عند انتهاء عمله مع الشــركة، أو في حالة نقل موظف إلى وظيفة أخرى داخل الشـــركة لا تتطلب مســـئولياتهم الجديدة الصـــلاحيات الحالية الممنوحة على هذه التقارير ، أو بناء على إخطار رســـمي من رئيس القطاع الذى يعمل به الموظف بتعديل الصلاحيات الممنوحة له.

مادة: (12)

التعديلات على برامج الأعمال أو تصميمات التقارير أو صلاحيات الإستخدام

يعد إستقرار برامج الأعمال وصلاحيات إستخدامها والتقارير التى تصدر من خلالها من الأمور التى يتوجب على قطاع تكنولوجيا المعلومات الحرص على إستمرارها، كما أن إجراء تعديلات على كلا من برامج الأعمال وتصميمات التقاريريتطلبان إجراءات موثقة ومعتمدة يراعى بها ما يلي من قواعد:

1- فى حاله حاجة أى قطاع لإجراء تعديل فى دورة عمل على برامج الأعمال أو بعض التقارير أو صلاحيات المستخدمين، يجب إعداد نموذج طلب تغيير ورقي او الكتروني ويعتمد من رئيس القطاع الطالب.

2- يجب أن يوضح بنموذج طلب التعديل أسباب التعديل، الجدول الزمنى المتوقع لإتمامه، ومعايير الاختبار، وعينة من النتيجة المتوقعة، قائمة بالمختبرين وخطة الإختبار وخطة إستعادة الوضع السابق قبل التغيير.

3- يقوم قطاع تكنولوجيا المعلومات مراجعة التعديل المطلوب على أن يعتمد رئيس قطاع تكنولوجيا المعلومات خطة التعديل أو رفضه وفقا للموازنة المتاحة والموارد المخصصة وترتيب الأولويات مع عرض رد قطاع تكنولوجيا المعلومات على القطاع الطالب، كما تناقش التعديلات المطلوبة مع قطاع المراجعة الداخلية لإبداء الرأي في نقاط الرقابة المقترحة و المطلوبة.

4- يقوم قطاع تكنولوجيا المعلومات ببحث إمكانية الاستعاضة بحلول بديلة للتعديل المطلوب من خلال البرامج المطبقة، أو التقارير المتاحة أو عمل تقارير جديدة أو خلافه.

5- فى حالة إقرار خطة التعديل فيقوم قطاع تكنولوجيا المعلومات بتطبيق التعديل حسب الطلب الذى تم الموافقة عليها علي بيئة اختبار، على أن يقوم مستخدمون من كافة القطاعات التى ترتبط بالتعديل المطلوب باتباع خطة الاختبار للتأكد من أن التغييرات التي تمت جيدة وتؤدي وظيفتها كما هو متوقع منها وليس لها أي تأثير سلبي علي القطاعات الأخرى.

6- بعد الوصول الي المستوي المرضي من القطاعات المختلفة على التعديل المطلوب فيتوجب على رؤساء القطاعات المعنيين بالتوقيع بقبول التعديلات، مع ضرورة إتفاق القطاع الطالب مع قطاع تكنولوجيا المعلومات على تحديد لتاريخ إدخال التغييرات محل التنفيذ الفعلى (مع ضرورة قيام القطاعات المشار إليها بتوثيق جميع التغييرات التي تمت على النظام).

7- أية تحديثات أو تطوير للبرامج طبقا لخطة سابقة الوضع (كما هو مبين بعاليه) سيتم تطبيقها في بيئة اختبار أولاً ويجب إخطار جميع أعضاء تطبيق العمل والمستخدمون المختارون لإجراء

الاختبارات اللازمة على التحديثات قبل تطبيقه حيث يتم شرح التغيير الذي طرأ والتاريخ المقترح فيه إجراء التغيير في بيئة الإنتاج الفعلية (كمبدأ عام فيما عدا الحالات التي يكون فيها التحديث ذا طابع طارئ أو ضروري، فسيمهل المستخدم النهائي فرصة أسبوعين لاختبار التحديث).

8- وفي حالة عدم إبلاغ قطاع تكنولوجيا المعلومات عن أي مشاكل قبل الموعد المقترح للتنفيذ في بيئة الإنتاج الفعلية، يتم تطبيق التحديث في موعده المحدد.

9- قد لا يسمح بإجراء اختبار على بعض التحديثات الحساسة من ناحية الوقت أو التي تعمل علي اصلاح عطل قبل تنفيذها في بيئة الإنتاج.

- وسيندرج ضمن هذه الفئة بعض التحديثات المالية أو التنظيمية أو القانونية.
- يمكن تطبيقها مباشـــرة على الإنتاج وفقا لتقدير رئيس قطاع تكنولوجيا المعلومات بالإتفاق مع رئيس القطاع الطالب والقطاعات المرتبطة بنفس البرنامج.

ثالثاً: الأمن المعلوماتى

مادة: (13)

تأمين البيانات وسياسة التوثيق والتصريح

يلتزم قطاع تكنولوجيا المعلومات بإتباع المعايير الضرورية بهدف توفير حماية فعالة تضمن تأمين جميع معلومات وأنظمة الشركة التي يمكن لموظفيها الوصول إليها عن طريق حساب للإستخدام أومن خلال الخدمات المقدمة على الفضاء السحابي (CLOUD) أو من خلال أى تواصل بشبكة الشركة، أو أى نظام له القدرة على تخزين أي معلومات تخصها غير مخصصة للنشر، ولتحقيق ذلك يتوجب الإلتزام بالإجراءات التالية:

1- يجب استخدام اجهزة الحاسب الآلى الخاصة بالشركة ووسائل الاتصال لأغراض العمل فقط، يتاح الاستخدام الشخصي المحدود (كما هو موضح فى بعض اللوائح الأخرى كلائحة إستخدام الهاتف المحمول على سبيل المثال).

2- يحتفظ قطاع تكنولوجيا المعلومات بالحق في الغاء صلاحيات أي مستخدم على أى نظام في أي وقت، ولا يسمح مطلقاً بأي تصرف يضر بأنظمة الشركة الألكترونية أو أى تصرف من شانه التأثير سلبياً علي قدرة استخدام الآخرين لها، كما لا يجوز أن يستغل أى مستخدم ضعف ونقص نقاط الرقابة وتأمين الأنظمة الألكترونية (إن تمكن من تحديده) لالحاق الضرر بهذه الأنظمة أو بالمعلومات المتاحة عليها أو للسعى للحصول على معلومات بشكل أكثر مما هو مصرح له به،

او لمحاولة الدخول إلي الأنظمة الأخرى التي لم يصـــرح له بالدخول عليها، بل على النقيض تتوقع الشركة من الموظفين ومستخدمى أنظمتها الألكترونية حال ملاحظتهم أي ضعف أو نقص فى نقاط تأمين هذه الأنظمة أو نقاط ضعف أن يقوموا بإرسال تقرير لقطاع تكنولوجيا المعلومات بشكل فوري.

3- في حال ترك أحد الموظفين العمل لدي الشـركة، يجب إلغاء جميع صـلاحياته الممنوحة له على أنظمة معلومات الشـركة فوراً، فيجب على المدير المباشـر ورئيس القطاع المعنى بالإتصـال والتنســيق مع قطاع الموارد البشــرية على الفور في حالة إنهاء عقد الموظف من أجل التنفيذ الفعلى لإلغاء صلاحياته على جميع أنظمة الشركة.

4- فى حال قررت الإدارة إنهاء عمل أحد الموظفين المؤقتين أو إنهاء التعاقد مع أي طرف أخر (إســتشــاريين، موردين، مقاولين ، مراجعين خارجيين ، الخ) يعمل لحســاب الشــركه وله صــلاحية الدخول على بعض أنظمتها المعلوماتيه، فيجب على القطاع المعنى الإبلاغ الفورى لقطاع تكنولوجيا المعلومات لإلغاء الصلاحيات المشار إليه.

5- فى حال نقل أحد الموظفين من إدارة/قطاع إلى إدارة/قطاع أخرفيتوجب على كلا الطرفين إبلاغ قطاع تكنولوجيا المعلومات لإعادة تحديث أو تغيير الصــلاحيات الممنوحة لهذا الموظف لتلائم احتياجات العمل بالإدارة الجديدة.

مادة: (14)

تصنيف سرية البيانات:

تقوم كل إدارة بتحديد تصنيف ما لديها من بيانات ومعلومات من ناحية مدى سريتها وتحديد من لهم حق الوصـول اليها. على ان يلتزم الموظفين المخول لهم الوصـول الى تلك المعلومات بعدم نقل هذه البيانات والمعلومات الى اي جهة او شـخص غير مخول له الحصـول على تلك المعلومات بأي طريقه او وسـيلة نقل معلوماتيه والأجراءات التالية توضــح ما ينبغى على الإدارات المختلفة إتباعه حيال نقل المعلومات شديدة السرية.

إجراءات نقل المعلومات شديدة السرية إلكترونياً:

الغرض من هذه الألية هو حماية المعلومات شديدة السرية بطريقة ملائمة قبل نقلها عن طريق الشبكات الداخلية أو الخارجية، ويجب تخصيص كلمه سر للدخول على الملف قبل نقله مستخدما تطبيقات مايكروسوفت أوفيس او أي أداة مشابهة ويرجى الرجوع لقطاع تكنولوجيا المعلومات للمساعده في تشفير تلك المعلومات قبل نقلها إذا اقتضت الحاجه.

مادة: (15)

ضوابط حماية أجهزة الحاسب الآلى المحمول

حيث أن جميع أجهزه الحاسب الآلى تواجه مخاطر أمن المعلومات، فإن أجهزة الحاسب الآلى المحمول تكون اكثر عرضه للتلف أوالفقد أو السرقة، وبالإضافة إلي ذلك، فإن حقيقة استخدامها خارج مقرات الشركة يزيد من تلك المخاطر (عرضة للتلف والفقد والسرقة سواء لإعادة بيعها أو طمعا في المعلومات التي تحتويها).

ولا تقتصر الخسائر أو المخاطر على قيمة استبدال الاجهزة المفقودة أو المسروقة أو التالفة وإنما يمتد الأثر لقيمة البيانات التي تحتويها أو إمكانية إستخدام هذه الأجهزة للوصول لبيانات أخرى من خلالها، فالمعلومات أصل هام للغاية للشركة، ولذا فقد حدد قطاع تكنولوجيا المعلومات الضوابط التالية لجميع مستخدمى أجهزة الحاسب الآلى المحمولة التى تعد مسئولية شخصية للموظف صاحب العهدة:

1- أن يحتفظ الموظف المختص بالحاسب المحمول به وعلي مرمي بصره كلما امكن، وأن يكون شديد الحذر في الأماكن العامة كالمطارات ومحطات السكة الحديد والمطاعم، فلا يحتاج السارق غير جزء من الثانية لسرقة كمبيوتر محمول غير معتني به.
2- أن يحتفظ الموظف بالحاسب المحمول في حقيبة مبطنه خاصة به أو في حقيبة مقواه لتقليل مخاطر التلف غير المقصود، وأن يتجنب إسقاطه أو خبطه، كما أن التخزين باستخدام الفقاعات الهوائيه يمكن أن يكون مفيدا، وينصح بحقيبة ذات مظهر عادي أفضل من الحقيبة المخصصة للحاسب المحمول لأنها أقل عرضه لجذب نظر السارق.

في حالة سرقة حاسب آلى محمول فينبغى أن يقدم الموظف تقرير حادث بواقعة السرقة بالتنسيق مع قطاع تكنولوجيا المعلومات في أسرع وقت ممكن علي ان لا يكون قد مر على الواقعة اكثر من 24 ساعة مرفقا بمحضر شرطه رسمي.

مادة: (16)

ضوابط إستخدام شبكة المعلومات الداخلية للشركة

عملية تسجيل الدخول أو تسجيل الخروج على الشبكة

يجب تحديد هوية جميع المستخدمين مسبقا قبل إستخدامهم نظم الاتصالات بالشركة ، فالدخول على الشبكة الداخلية للشركة يتطلب إدخال اسم المستخدم مع كلمة سر ثابتة ويشترط أن إسم المستخدم وكلمة السر كلاهما يميز مستخدم واحد فقط، ويحظر تسجيل دخول المستخدمين للنظام أو شبكة الشركة بدون اسم المستخدم (مثلا باستخدام هوية "زائر").

أمن شبكة المعلومات الداخلية

يجب على كل مستخدم إبلاغ قطاع تكنولوجيا المعلومات فورا عن أي اشتباه في مشكلة بأمن الشبكة، على سبيل المثال حالات الإختراق.

وتعدالبيانات عن التدابير الأمنية لأنظمة الكمبيوتر والاتصالات الخاصة بالشركة من نوعية "سرية" ، ويحظر الإفصاح عنها لمن ليس لديهم إذناً بذلك من رئيس قطاع تكنولوجيا المعلومات.

. يجب على المستخدمين عدم إجراء آية محاولات لإختبار أو محاولة الكشف عن الإجراءات الأمنية لأنظمة الحاسب أو الاتصالات أو الشبكات، الخ إلا إذا تمت الموافقة كتابيا علي ذلك بشكل مسبق من رئيس قطاع تكنولوجيا المعلومات ، وأي حدث ينطوي على اختراق غير مسموح به للنظام أو كلمة السر(التخمين) أو فك تشفير الملفات أو الغش في نسخ البرمجيات أو محاولات مشابهه غير مصرح بها للكشف عن الإجراءات الأمنية فهي كلها أفعال غير قانونية، وسيتم اعتبارها إنتهاكات خطيرة ويتعرض مرتكبوها لعقوبات حسبما تقرره الإدارة طبقاً للوائح الشركة.

قواعد تغيير كلمة السر

جميع كلمات السر على مستوى اعدادات النظام وينفذها مديري الأنظمة التكنولوجية، مثل كلمات المرور هذه يجب تغييرها بشكل نصف سنوي على الأقل.

جميع كلمات السر على مستوى المستخدم (على سبيل المثال، البريد الإلكتروني والإنترنت والكمبيوتر المكتبي، إلخ...) يجب تغييرها على الأقل كل ستة أشهر.

لمديري الأنظمة التكنولوجية إستخدام حساب مستخدم عادى (كأى مستخدم بالشركة) كما يجوز منحهم حق إضافة مستخدم أخر للدخول على أنظمة الشركة بإسم وكلمة مرور مختلفة بحكم صلاحيات إدارتهم لهذه الأنظمة.

إرشادات خاصة بتكوين كلمة السر

ينبغي على كافة العاملين في الشركة أن يكونوا على وعي بكيفية عمل كلمة سر يصعب تخمينها.

وتتميز كلمة السر القوية بالآتي:
تحتوي على ثلاثة على الأقل من المواصفات الخمسة التالية:

- أحرف صغيرة إنجليزية
- أحرف كبيرة إنجليزية

- أرقام
- علامات ترقيم
- "رموز خاصة" (مثل @#$%^&*()_+|~-=\`{}[]: ";'<>/ وغير ذلك.)
- تحتوي على ما لا يقل عن ثمانية أحرف أبجدية ورقمية.

اما كلمة السر الضعيفة فتتسم بالتالي:

- تحتوي على أقل من ثمانية أحرف
- كلمة موجودة في القاموس (الإنجليزي أو باللغات الاخري)
- كلمة شائعة الاستخدام مثل:
- أسماء اعضاء الأسرة، والحيوانات الأليفة، والأصدقاء، وزملاء العمل، والشخصيات الخيالية، الخ...
- شروط وأسماء أجهزة الكمبيوتر والأوامر ومواقع وشركات والأجهزة والبرمجيات.
- أعياد الميلاد وغيرها من المعلومات الشخصية مثل العناوين وأرقام الهواتف.
- كلمة أو نمط مثل aaabbb، qwerty ، zyxwvuts ،123321 ، الخ...
- أي مما سيبق ذكرة مكتوب بالعكس.
- أي مما سبق ذكرة مسبوق أو يليه أرقام (على سبيل المثال، secret1،1secret).

معايير حماية كلمة السر

- يفضل دائما استخدام كلمات سر مختلفة لحسابات الشركة عن كلمات السر المستخدمة للحسابات الشخصية.
- استخدم دائما كلمات سر مختلفة للدخول للأنظمة المتعددة بحسابات الشركة كلما أمكن. على سبيل المثال، حدد كلمة سر واحدة للأنظمة التي تستخدم خدمات الدليل (LDAP والدليل النشط وغير ذلك) أو التوثيق و كلمة سر أخرى لتسجيل الدخول على برامج SAP وهكذا.
- لا تشارك كلمات السر الخاصة بالشركة مع أي شخص بما فيهم المساعدين الإداريين والسكرتارية، كما يجب أن تعامل كافة المعلومات الخاصة بكلمة السر على أنها معلومات حساسة وسرية.
- لا ينبغي أن تكتب كلمات السر أو يتم تسجيلها على الانترنت دون تشفير.
- لا تكشف كلمة السر في رسالة الكترونية أو عن طريق الدردشة أو غير ذلك من وسائل التواصل الالكتروني.
- لا تتحدث عن كلمات السر أمام الآخرين.
- لا تعطي أية تلميحات بشأن شكل كلمة المرور (مثل "لقب الاسرة").
- لا تكشف عن كلمة السر الخاصة بك في أى استبيانات.
- إذا طلب منك أحدهم كلمة السر، شر إلى هذه الوثيقة وأرشدهم إلى قسم أمن المعلومات.
- يجب إبلاغ قسم الأمن المعلوماتي في حالة الاشتباه في إختراق الحساب أو كلمة السر.

مسؤوليات مستخدمى شبكة المعلومات الداخلية

مستخدمي شبكة المعلومات الداخلية هم الأفراد الذين تم منحهم إذن / تفويض صريح لتسجيل الدخول، وتعديل أو مسح أو الإستفادة من معلومات تخص الشركة بموافقة رئيس القطاع المعنى بالبيانات ، ويجب ان يتعامل المستخدمين مع تلك المعلومات فقط للأغراض التي تم الموافقة عليها من قبل رئيس القطاع المعنى ، كما يتعين على المستخدمين الإمتثال التام لقواعد الأمان والحماية الموضحة في هذه اللائحة وأى لوائح أخرى تخص القطاع المعنى.

يجب ان يمتنع المستخدمين من كشف أو التصريح بالمعلومات التي في حيازتهم (الا إذا تم تصنيفها كمعلومات عامة) وذلك دون اذن مسبق من رئيس القطاع المعنى، كما أن تخزين اي بيانات خاصة بالعملاء بشكل شخصى او فى الهواتف النقالة هو فعل غير مصرح به بتاتا، ويجب ان يقوم المستخدمين بإبلاغ قطاع تكنولوجيا المعلومات فورا إذا كان لديهم اعتقاد أو اشتباه في ضعف أو اختراق أمني لأية معلومات.

مادة: (17)

ضوابط الحماية ضد الفيروسات والإختراق

يلتزم قطاع تكنولوجيا المعلومات بالشركة بأن تكون جميع أجهزة الحاسب الآلى بالشركة بكافة أنواعها التى تتصل بشبكة المعلومات الداخلية بمعايير حماية موحدة ومدعومة ببرامج مكافحة الفيروسات والتى تعمل وفق فترات منتظمة.

أما بخصوص تلك الأجهزة التى تعمل فى قطاعات أخرى وغير خاضعة لقطاع تكنولوجيا المعلومات (أجهزة خطوط الإنتاج أو أجهزة الميكنة وخلافه) و بسيرفراتها فيتوجب على رئيس القطاع المعنى تدبير إجراءات الحماية الواجبة لهذه الأجهزة طبقاً لهذه اللائحة ويجوز لقطاع تكنولوجيا المعلومات تقديم الدعم الفنى اللازم فى حال طلبه.

ولقطاع تكنولوجيا المعلومات فى حال رصد أى مخاطر على آياً من أجهزة الشركة برفع تقرير لرئيس القطاع المعنى والرئيس التنفيذى لقطاعات الدعم لإتخاذ ما يلزم. المختلفة، على الجميع الإلتزام ب ، و يلتزم قطاع تكنولوجيا المعلومات والقطاعات المشار إليها بعاليه أو ما فى حكمها بالإلتزام بما يلي:

1- أعمال التحديث الدورية و المستمرة لبرامج مكافحة الفيروسات.
2- تحديد الاحتياجات الفنية والاحتياطات الواجب الوفاء بها من قبل جميع مستخدمي أجهزة الكمبيوتر التي ترتبط أو قادره على الاتصال بشبكة معلومات الشركة،

3- ضـمان فعالية الكشـف عن الفيروسـات وبرامج التجسـس، وبرامج الإعلانات الخبيثة، وكيفية الحماية منها.

ولقطاع المعلومات فى ذلك إتباع الإجراءات التالية:

1- تثبيت برامج الحماية من الفيروسات على جميع الأجهزة المملوكة للشركة.
2- وفي حالة وجود جهاز أو أجهزة مصابة بالفيروس، يجب أن يتم فصلها وعزلها عن الشبكة حتى يتم تأكيد خلوها من الفيروس.
3- ويعد موظفوا قطاع تكنولوجيا المعلومات دون غيرهم هم المسؤولون عن عمل الإجراءات التي تكفل عمل البرمجيات المضـادة للفيروسـات وأداء المسـح المنتظم، حتى يتم التأكد ان الأجهزة المتصلة بشبكة الشركة خالية من الفيروسات.
4- رصد اي نشاط يهدف إلى نشر او انشاء برامج ضارة أو ملفات مصابة على شبكة الشركة (مثل الفيروسات أو تروجان أو الايميلات الضارة وغير ذلك) ورفع تقارير للرئيس التنفيذى لقطاعات الدعم والسيد العضو المنتدب.

وتحمل الشركة العاملين بها مسئولية اتخاذ الإجراءات الإحترازية عند إتمام تبادل البيانات والمعلومات بأن يتم ذلك من خلال مصادر موثوقة ، وتجنب أية طرق اتصال مشبوهة، والتاكد من المسح الكامل لأية وسائل تخزين خارجية (مثل الفلاش ميمورى) قبل إستخدامها.
فى حال أضطر الموظف إلى استخدام أجهزة الكمبيوتر الشخصية فى ظروف طارئة للدخول على شبكة المعلومات الداخلية للشركة, فعليه التنسيق مع قطاع تكنولوجيا المعلومات لضمان الحماية الواجبة.
كما تقع مسئولية إبلاغ قطاع النظم في حالة الإصابة بفيروس الكتروني أو الاشتباه في الإصابة علي عاتق المستخدمين بصفة فورية مع فصل الجهاز من الشبكة فورياً.

مادة: (18)

ضوابط عمل النسخة الاحتياطية واستعادة البيانات عند الحاجة

تنطبق هذه الضوابط على سيرفرات محددة، وبرامج تطبيقات الأعمال، وقواعد البيانات، بيانات المستخدمين أفراد ومجموعات والتقارير الخاصة بالأعمال التي يجب حفظها وفقا لمتطلبات الحفظ العامة والخاصة بالشركة والتى تحددها القطاعات المختلفة بالتنسيق مع قطاع تكنولوجيا المعلومات.

وتنطبق على المستخدمين من العاملين المصرح لهم بالإتصال بشبكة المعلومات الداخلية للشركة من خلال أجهزة الحاسب الآلى التى تمتلكها ولا تغطي البيانات أو الأجهزة الشخصية.

يتخذ قطاع تكنولوجيا العملومات الإجراءات والتدابير اللازمة لتوفير الأجهزة والبرامج والتكنولوجيات التي تسمح بعمل نسخ احتياطية داخل الشركة وخارجها وتحديد بيانات العمل الهامة والحرجة والتطبيقات وقواعد البيانات الواجب حفظها.

ولا تشمل هذه التدابير فقط على مكتبات التسجيل الافتراضية والمادية والاقراص الصلبة، وبرامج الحفظ والإستعادة ومستلزماتها والتي يمكن الاعتماد عليها وتم إختبارها و التحقق من ادائها.

ويحدد قطاع تكنولوجيا المعلومات أوقات الحفظ والمدد الزمنية بين كل عملية حفظ وأخرى، وإجراءات الإحتفاظ بالنسخ الإحتياطية والمدد المطلوبة للإستعادة عند الحاجة ومواقع الحفظ وأدواته والتفصيلات الأخرى الفنية المرتبطة به.

مادة: (19)

ضوابط إستخدام التليفون المحمول للدخول على الشبكة لموظفى الشركة وزوارها

تسمح الشركة لموظفيها أو لبعض الزائرين الراغبين في الدخول على شبكتها المعلوماتيه لأغراض العمل ضمن تعاقد، بإستخدام التليفون المحمول فى الدخول على شبكة المعلومات الداخلية من خلال عدد من الضوابط والقيود التالية:

والأجهزة التى من الجائز إستخدامها أجهزة الكمبيوتر اللوحي مثل الآيباد، أجهزة المحمول / الهواتف الخلوية، الهواتف الذكية وأجهزة PDA

1- يحتفظ قطاع تكنولوجيا المعلومات بالحق في رفض توصيل الأجهزة المحمولة إلى الشبكة الخاصة بالشركة سواء كان بشكل مادي أو غير مادي، ولقطاع تكنولوجيا المعلومات عند رصد استخدام هذه المعدات بطريقة تضع أنظمة الشركة أو البيانات أو الموظفين أو معلومات الشركة في خطر ان تتخذ اجراءات رفض الإتصال وقطعه.
2- تعد موافقة رئيس القطاع المعنى مع توضيح حاجة العمل شرطًا أساسيًا لإعتماد قطاع تكنولوجيا المعلومات للدخول على الشبكة من خلال أجهزة المحمول بالنسبة للزائرين.
3- قبل الاستخدام الأولي على شبكة الشركة أو اي بنية تحتية اخري، يجب أن يتم تسجيل جميع الأجهزة المحمولة مع قطاع تكنولوجيا المعلومات.

4- يحتفظ قطاع تكنولوجيا المعلومات بقائمة تتضمن الأجهزة المحموله التي حصلت على الموافقات المطلوبة؛ أما الأجهزة غير الموجودة على هذه القائمة فلا تمنح حق للإتصال بشبكة الشركة.
5- يحصل المستخدمون فقط المعلومات الضرورية لأداء دورهم عبر هواتفهم المحمولة، وذلك لأسباب أمنية بحتة مثل سرقة المحمول أو القرصنة.
6- يجب على المستخدمين الإبلاغ عن الأجهزة المفقودة أو المسروقة لقطاع تكنولوجيا المعلومات التابع للشركة على الفور من أجل مسح الجهاز من قائمة الأجهزة المصرح لها تسجيل الدخول.
7- إذا تشكك مستخدم من حدوث دخول غير المصرح به إلى بيانات الشركة عبر جهاز محمول فيجب على المستخدم إبلاغ قطاع تكنولوجيا المعلومات لإتخاذ اللازم.
8- يجب أن لا تكون الأجهزة مرت بعملية "كسر الحماية أو فك شفرة"* أو تحتوي علي أي من البرمجيات الغير القانونية أو المثبتة والتي صممت للوصول إلى وظائف غير مصرح بها.
9- لا يجوز للمستخدمين تحميل البرامج المقرصنة أو تلك التي تتضمن محتوى غير قانوني على أجهزتهم.
10-يجب أن يتم تثبيت التطبيقات من منصة مالك المصادر الرسمية المعتمدة، ويحظر تثبيت اكواد برامج من مصادر غير موثوق بها.
11-يجب أن تبقى الأجهزة محدثة طبقا للتحديث الذي يتيحة مصنع الجهاز.
12-لا يجوز ربط أو وصل الأجهزة المحمولة بأجهزة الكمبيوتر التي لا تحتوي علي اخر تحديث متاح أو تلك التي لم يثبت عليها مضاد للفيروسات أو الحماية من البرامج الضارة.
13-يجب أن يتوخى المستخدمون الحذر بشأن دمج حسابات بريدهم الإلكتروني الشخصي والخاصة بالعمل على أجهزتهم، كما يجب إيلاء عناية خاصة لضمان عدم إرسال بيانات الشركة إلا من خلال نظام البريد الإلكتروني الخاص بالشركة فقط.
14-لا يجوز لمستخدمين استخدام أجهزة العمل لتخزين نسخ احتياطيه أو مزامنة المحتوى من ملفات إلا إذا كان قانونيا وبهدف مشروع للعمل يحدده قطاع تكنولوجيا المعلومات.

يلتزم الموظف بالتأكد من أن جهاز المحمول خاصته يحتوي علي برامج مكافحة الفيروسات الصالحة والمحدثة، وفى حالة رصد قطاع تكنولوجيا المعلومات لأى مخالفة يرفع تقريراً للرئيس التفيذى لقطاعات الدعم لإتخاذ ما يلزم تجاه المخالفة مع قطع الإتصال مع الشبكة عن هذا الجهاز.

مادة: (20)

ضوابط تحديث أجهزة الحاسب الآلى و الإستبعاد

لقطاع تكنولوجيا المعلومات إتخاذ التدابير اللازمة بعد موافقة السـلطة المختصـة من أجل الحفاظ على أعلى مسـتوى من إسـتمرار الأنظمة الألكترونية بالخدمة دون تعطل وذلك بالحفاظ على كافة الأجهزة الملائمة للعمل وصيانتها بما في ذلك أجهزة الحاسب على إختلاف أنواعه والبرامج المناسبة الضرورية لتوصـيل المعلومات، ومواكبة التغيرات السـريعة في التكنولوجيا والذى يتطلب وجود خطة معتمدة لتطوير واستبدال أجهزة الحاسب الآلى والسيرفرات وأجهزة الشبكة والطابعات والماسحات الضوئية والأجهزة الملحقة وغيرها من التكنولوجيات لضمان إستمرار عمل الأنظمة الألكترونية وأن تظل متاحة للخدمة لتحقيق أهداف الشركة.

ويحدد الجدول التالى توصـيات قطاع تكنولوجيا المعلومات لمعدلات الإحلال والتجديد الواجب إتباعها بعد موافقة السلطة المختصة وتوافر الموازنة المعتمدة لذلك:

نوع الأجهزة	الاستخدام الموصى به ثم الإحلال
أجهزة الاتصالات	5 سنوات
السيرفرات	5 سنوات
أجهزة الكمبيوتر المكتبية	5 سنوات
أجهزة الكمبيوتر المحمولة	4 سنوات
شاشات LCD LED	5 سنوات
أجهزة الملحقة (مثل: الطابعات والطابعات متعددة الوظائف و الماسحات الضوئية وأجهزة العرض، إلخ....)	4 سنوات
البرامج	يتحدد الاستخدام الموصى به للبرامج بشكل منفصل طبقا لنوع البرنامج وحاجته للتحديث او التغيير.

ضوابط الإحلال والتجديد:

1- عند إجراء تحديث أو الإحلال والتجديد لجهاز حاسب آلى، فيجب رد الجهاز القديم لقطاع تكنولوجيا المعلومات للإعداد لعملية التخلص منه، وفقًا للوائح الخاصة بهذا الشأن.
2- لا يجوز إعادة استخدام الأجهزة القديمة التي تم تحديثها أو تلك المخلفة عن عملية الإحلال والتجديد من أجل تجنب تدهور الخدمات والتعطيل.
3- ينبغي أن تمسح كافة البيانات الموجودة على الأجهزة القديمة من خلال أدوات يحددها قطاع تكنولوجيا المعلومات.
4- على الرغم من أن معظم أجهزة الحاسب الآلى المملوكة للشركة مشمولة بعقود صيانة إلا أنها لا تقوم بتغطية سوء الاستخدام، لذا فهي مسئولية المستخدم أن يقوم بحماية الأصل المعين له

من قبل قطاع تكنولوجيا المعلومات بما في ذلك أجهزة الحاسب الآلى المكتبية أو أجهزة الحاسب الآلى المحمولة أو تليفون مكتبي من الضرر الناتج عن سوء الاستخدام.

رابعاً: الخدمات والدعم الفنى

مادة: (21)

طلب خدمة ودعم تكنولوجيا المعلومات

يقدم قطاع تكنولوجيا المعلومات الدعم الفني لموظفى الشركة فقط ولما تملكه الشركة من أجهزة وبرامج تطبيقات الأعمال وبالتالي لا يسمح لموظفي قطاع تكنولوجيا المعلومات تقديم دعم لأية أجهزة شخصية أو برمجيات غير موافق عليها تحت اي ظرف من الظروف, وتقدم خدمات الدعم الفنى من خلال الإجراءات التالية:

1- ينبغي أن تطلب الخدمات والدعم الفني من خلال القنوات المعتمدة (والتي تشمل خدمات تكنولوجيا المعلومات وانظمة التطبيقات من إدارة الدعم الفني ومراكز الاتصال المعلن التابعة لتكنولوجيا المعلومات).
2- مركز الاتصال عبر الهاتف لتكنولوجيا المعلومات يستخدم عند حدوث خلل أو طلب دعم للنظام في حالة توقف عمله أو تعطله أما في غير تلك الحالات فينبغي على الموظف تقديم طلب للدعم من جهاز الكمبيوتر الخاص بهم إلى أنظمة/بوابة خدمة مكتب الدعم الفني.
3- ينبغي أن يتضمن طلب الدعم الفني وتقديم الخدمات بطاقة تعريف الموظف واسم القسم ومركز التكلفة ووصفًا واضحا للخدمة المطلوبة أو المشكلة المبلغ عنها.
4- يجب ان يتم تحديد أولوية طلب الدعم الفني وتقديم الخدمات على مقياس الأولوية طبقا لتاثيره على سير العمل وطبيعة المشكلة وعدد المستخدمين المتضررين.
5- أما بالنسبة للدعم أو طلب الخدمة العادية (التي تؤثر على موظف واحد) فتحدد الأولويه بشكل رئيسى على أساس من يأتي أولاً يخدم أولاً ووفقًا لموارد قطاع تكنولوجيا المعلومات.