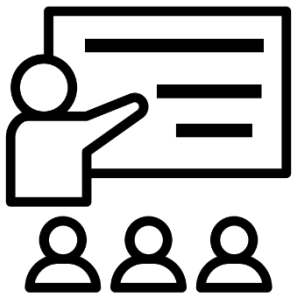
GROWTH BYTES

دليل سياسات

الدعم التقني – IT Technical Support

قطاع صيانة المباني



قائمة المحتويات

الدعم التقني IT Technical Support

1. المقدمة والمبادئ العامة

تشبه البنية التحتية لتكنولوجيا المعلومات البنية التحتية في أي مدينة، من حيث أنها تتكون من مكونات مادية ومكونات خدمية تدعم الأنشطة التي يطلبها المستخدمون لدعم وظائف الأعمال. هناك تطبيقات تدعم الوظائف الرئيسية وهناك الخوادم التي تستضيف تلك التطبيقات ومراكز للبيانات خاصة بها.

هناك أيضًا بنية تحتية للشبكات تسهل الوصول إلى التطبيقات والخوادم للأعمال، وبالتالي يشير مصطلح البنية التحتية لتكنولوجيا المعلومات إلى جميع المكونات والعناصر التي تدعم شبكة ربط الأجهزة ببعضها وبالانترنت ووظائف الإدارة والوصول للبيانات والمعلومات.

تُشرف إدارة البنية التحتية لتكنولوجيا المعلومات على عناصر المعلومات الرقمية الأساسية المطلوبة لتقديم خدمات الأعمال. يمكن أن يشمل ذلك تطبيقات البرامج والمكونات المادية للشبكات، ولكن التركيز الأساسي لإدارة البنية التحتية لتكنولوجيا المعلومات ينصب عادةً على المكونات المادية مثل أجهزة الكمبيوتر والشبكات التي تساند ذالك.

يعتمد فهمنا لإدارة البنية التحتية لتكنولوجيا المعلومات على المعرفة بالمكونات المحددة للبنية التحتية لتكنولوجيا المعلومات والمهام الأكثر أهمية المرتبطة بإدارة كل مكون، وبالتالي تنقسم إدارة البنية التحتية لتكنولوجيا المعلومات أحيانًا إلى ثلاث فئات فرعية وهي: إدارة الأنظمة وإدارة الشبكة وإدارة تخزين البيانات وإدارة البنية التحتية.

إدارة الأنظمة

من المهم ان تشمل إدارة الأنظمة، إدارة جميع أصول تكنولوجيا المعلومات الموجودة، ويكون مسؤولي المعلومات أو المسؤولين التقنيين هما مسؤلان عن الإشراف على العمليات اليومية لمركز البيانات والبنية التحتية وإدارة تكامل التطبيقات الجديدة والخدمات المقدمة من الجهات الخارجية Third Party Services في بيئة تكنولوجيا المعلومات للمؤسسة.

وتشمل أنشطة إدارة الأنظمة أيظاً أمن الشبكات، مثل كشف أي تسلل خارجي والوقاية منه، ومعلومات الأمان وإدارة كافة الأحداث المتعلقة بتلك الأنظمة، وكذلك تندرج إدارة السجلات وأتمتة عبء العمل وتكامل التطبيقات والخدمات تحت إدارة الأنظمة

إدارة الشبكة

يجب على محللو عمليات وأمن تكنولوجيا المعلومات إدارة الشبكات وتكوينها لضمان تخصيص الموارد بشكل صحيح للتطبيقات والخدمات عند الحاجة، والحفاظ على جودة خدمات الشبكة وتوفرها. تتضمن إدارة الشبكة أيضًا عنصرًا من عناصر الأمان، حيث يجب على مشغلي تكنولوجيا المعلومات الحفاظ على الرؤية والشفافية في الشبكة للتحكم في الوضع الأمني للمؤسسة والحماية من الوصول غير المصرح به وخروقات البيانات.

ادارة التخزين

إن أحد الجوانب الهامة لإدارة البنية التحتية لتكنولوجيا المعلومات هو الإشراف على تقنيات وموارد تخزين البيانات. تعد مساحة تخزين البيانات أحد الأصول المحدودة والقيمة للمؤسسات. لذلك يجب إدارة مثل توفر التخزين، وضغط البيانات، وأمن البيانات والسيرفرات بدقة متناهية.

من أهم مسؤوليات إدارة التخزين:

- ضغط وفهرسة البيانات
- توفير التخزين التلقائي
- اخذ نسخ احتياطية للبيانات (Backup)
- توفير منصة امنة لحفظ البيانات (على السحابة الرقمية والأقراص الصلبة في ان واحد)
- إدارة برامج امن وسلامة البيانات وتحديثها باستمرار للحماية من فقدان البيانات أو سرقتها.
- العمل المستمر على تقليل وقت معالجة البيانات والدخول اليها(Access time).

2. اجزاء البنية التحتية لتكنولوجيا المعلومات IT Infrastructure Componenets

يتحمل مشرف البنية التحتية لتكنولوجيا المعلومات مسؤولية تصميم وصيانة وتشغيل وإيقاف كل عنصر من عناصر البنية التحتية لتكنولوجيا المعلوماتا:

منصات أجهزة الكمبيوتر

تشمل أجهزة الكمبيوتر على أجهزة العميل مثل أجهزة الكمبيوتر المحمولة وأجهزة كمبيوتر سطح المكتب إلى جانب أجهزة الخادم والحواسيب المركزية.

أنظمة التشغيل الأساسية (operating systems)

تعد أنظمة التشغيل التي تعمل على الأنظمة الأساسية لأجهزة الكمبيوتر هي المكون الثاني للبنية التحتية لتكنولوجيا المعلومات. تشمل أنظمة التشغيل الشائعة Windows و UNIX و Linux و Mac OS X.

من المهم جداً ملاأمة أنظمة التشغيل للعمل المراد معالجته، فعلى سبيل المثال تجد أن نظام التشغيل Mac OS هو الأمثل لمعالجة المرئيات والتصميم الجرافيكي وبالمقابل تتم معالجة وفهرسة البيانات الكبرى على نظام تشغيل Linux في أغلب الاحيان.

تطبيقات البرمجيات

يجب ان تركز إدارة البنية التحتية لتكنولوجيا المعلومات على إدارة المكونات المادية للبنية التحتية لتكنولوجيا المعلومات، وتمارس الإشراف على أهم تطبيقات برامج دعم البنية التحتية للمؤسسة. وهي التطبيقات التي تعتبر بالغة الأهمية لإدارة تقديم الخدمات على مستوى المنظومة، مثل SAP و Oracle و Microsoft وغيرها.

إدارة البيانات وتخزينها

تعد الإدارة والإشراف على مكونات تخزين البيانات إحدى الوظائف الرئيسية لإدارة البنية التحتية لتكنولوجيا المعلومات. قد تكون مؤسسات تكنولوجيا المعلومات مسؤولة عن إدارة المكونات المادية لتخزين البيانات، مثل خوادم البيانات، جنبًا إلى جنب مع مكونات البرامج المستخدمة لتنظيم قواعد البيانات (MySQL و IBM DB2 و Oracle وغيرها).

منصات الشبكات والاتصالات

تندرج الشبكة الداخلية للشركة ضمن اختصاص إدارة البنية التحتية لتكنولوجيا المعلومات لتغطي كل شيء بدءًا من برامج الشبكة الافتراضية (خادم Microsoft Windows و Cisco وما إلى ذلك) إلى البنية التحتية المادية للاتصالات (الهواتف وأجهزة التوجيه والأسلاك والشبكات الاسلكية وما إلى ذلك)

الإنترنت

ترتبط البنية التحتية المتصلة بالإنترنت ارتباطًا وثيقًا بمكونات الشبكات والاتصالات السلكية واللاسلكية في البنية التحتية لتكنولوجيا المعلومات. تعد مواقع الويب المستضافة على خوادم داخلية أو خارجية وتطبيقات الويب وأدوات تطوير برامج الويب وخدمات استضافة الويب جزءًا من البنية التحتية لتكنولوجيا المعلومات.

خدمات الاستشارات وتكامل النظام

قد تشارك المؤسسة في أعمالها التجارية التي تستخدم الأنظمة القديمة في تنفيذ بنية تحتية جديدة لتكنولوجيا المعلومات لتحديث الأنظمة القديمة بتطبيقات جديدة أكثر قوة وقوة للإعداد التكنولوجي الحديث، وبالتالي تحتاج إلى شراء خدمات استشارية أو أنظمة من طرف ثالث.

أهم ممارسات إدارة البنية التحتية لتكنولوجيا المعلومات

نظرًا لأن المعنيين بالبنية التحتية لتكنولوجيا المعلومات مسؤولون عن التصميم والتنفيذ والصيانة لكل عنصر من عناصر البنية التحتية المذكورة أعلاه، فمن الضروري فهم أفضل الممارسات لإدارتها، التي تتظمن ما يلي:

- جمع المعرفة: تحديد متطلبات الأعمال الفنية والتقنية بهدف تصميم أفضل الحلول للبنية التحتية.
- إنشاء المعايير: تحديد آليات العمل المناسبة وتدريب كافة المستخدمين عليها.
- تنفيذ المعايير: متابعة تطبيق المعايير وتصحيح الأخطاء والتواصل مع جميع المستخدمين.
- الحفاظ على المعايير: أي تطبيق تلك المعايير المعتمدة بعيدا عن أي أهواء شخصية أو محاباة.
- التوثيق: الاحتفاظ بكافة المواصفات الفنية للأنظمة وتفاصيل مُزويديها وأرشفة سجلاتها.

فوائد إدارة البنية التحتية لتكنولوجيا المعلومات

تتلخص فوائد الإدارة الجيدة للبنية التحتية لتكنولوجيا المعلومات في تحقيق الوفر المالي والتشغيلي، منها:

- أوقات استجابة محسنة للتغيرات في العمليات، والكوارث، وأي ظروف أخرى.
- تدابير استباقية نابعة من عمليات أكثر رشاقة.
- انخفاض التكاليف المالية من الأتمتة.
- تبسيط عمليات ومسؤوليات الموظفين لخلق كفاءات العمل ورفع الانتاجية.
- تقليل وقت تعطل التطبيقات والأنظمة

3. مكونات البنية التحتية IT Infrastructure Componenets

جزء رئيسي من البنية التحتية للشركة هو تحديد المتطلبات وبالتالي تحديد المكونات الضرورية للبنية التحتية والعمل على شراءها وتطبيقها. فيما يلي المكونات الرئيسية للبنية التحتية وأهميتها ومقتضيات استخدامها:

متطلبات الأجهزة والبرامج

لا يوجد حل وحيد وشامل يمكن تطبيقه على جميع الشركات الصغيرة والمتوسطة. تختلف احتياجات الشركات، وكذلك وظائف تكنولوجيا المعلومات الخاصة بهم.

يجب عليك تخطيط متطلباتك واختيار المنتجات المناسبة التي تحل مشاكل عملك. نظرًا لأن الشركات تتطلب أجهزة وبرامج متعددة، فأنت بحاجة إلى التأكد من توافقها مع بعضها البعض وتوافقها مع متطلبات العمل كذلك.

تتطلب الأعمال التجارية المختلفة أدوات برمجية مختلفة للتعامل مع عملياتها الأساسية؛ على سبيل المثال، تحتاج شركة تصنيع إلى برنامج إدارة المخزون (Inevntory Management System) ، والذي يمكن أن يكون ذا فائدة قليلة لشركة محاسبة.

تذكر. يجب ان تخطط متطلبات البنية التحتية بشكل استراتيجي لتحصل ميزة تنافسية في مجال عملك، ولذلك فمن الاهميةأن يؤخذ في الاعتبار كل شيء من عدد المستخدمين إلى متطلبات حجم تخزين البيانات وغيرها.

نسبة استيعاب الخادم إلى محطات العمل

يجب امتلاك خادم للشركات التي لديها أكثر من خمس محطات عمل أو حواسيب. بدون خادم، لا تستطيع محطات العمل الخاصة بك وحدها التعامل مع عبء العمليات التجارية اليومية. على سبيل المثال، إذا كان لديك نشاط تجاري للتسوق عبر الإنترنت، فإن العدد الهائل من الأمور الأمنية والفواتير يمكن أن يطغى على محطات العمل وعلى نظام تكنولوجيا المعلومات لديك.

إعداد الخادم ليس مكلفًا، حتى بالنسبة للشركات الصغيرة. على الرغم من أن خادمًا واحدًا يمكنه التعامل بسهولة مع أكثر من 10 مستخدمين، فمن الأفضل قصر عدد المستخدمين على 10 لضمان الأداء الأمثل. كذلك يمكن استخدام البيئة السحابية واستعمالها كخادم كما هو دارج الان

أداء الشبكة

يعد أداء الشبكة أمرًا بالغ الأهمية للعملياتها التجارية نظرًا لتأثيرها المباشر على العمليات وبالذات للشركات الصغيرة والمتوسطة حيث يؤثر أداء الشبكة الضعيف على إنتاجيتها، ويساهم في وقت تعطلك، ويتكبد تكاليف باهظة. يمكن تجنب ذلك من خلال الاستثمار في معدات أجهزة الشبكات المناسبة واتصال إنترنت سريع.

التخزين والأمان

أثمن سلعة في القرن الحادي والعشرين هي البيانات. (Data is the new oil) وبالتالي، تنفق الشركات الكبيرة مليارات الدولارات كل عام في تخزين البيانات ومعالجتها وأمانها. البيانات مهمة لجميع الشركات.

يجب أن تجد أفضل طريقة لتخزين بياناتك. ان استخدام محركات الأقراص الثابتة والتخزين السحابي أو مراكز البيانات -حسب حجم عملك واحتياجات التخزين- هو امر في غاية الأهمية.

من المهم الاستثمار في خدمات استمرارية الأعمال المستندة إلى السحابة واستعادة البيانات بعد الكوارث لبياناتك الهامة.

يجب دمج حلول أمان المؤسسة المتوافقة مع احتياجات عملك. ومن المهم أن تحمي الشركات الصغيرة والمتوسطة نقاط النهاية والشبكات والخوادم وأنظمة العملاء. لدمج هذا بنجاح.

يجب على الشركات الاستثمار في جدران الحماية (Firewall)وحلول مكافحة الفيروسات وأنظمة المصادقة متعددة العوامل(Ports) والمزيد.

العوامل الرئيسية في بناء البنية التحتية

- استخدم الحلول القابلة لزيادة الحجم في المستقبل(Network updates and capacity)

يجب أن تكون الحلول التي تستخدمها قادرة على الحفاظ على نموك المستقبلي. على سبيل المثال، الحلول المستندة إلى السحابة قابلة للتطوير بسهولة، حيث يمكنك إضافة المزيد من الوظائف عندما تزداد متطلباتك. ابحث عن حلول لا تسبب أي ضغط في قسم تكنولوجيا المعلومات لديك مع نمو متطلبات عملك.

- اختر الموردين المناسبين: تقوم معظم الشركات الصغيرة والمتوسطة بالاستعانة بمصادر خارجية لخدمات تكنولوجيا المعلومات الخاصة بها لمزودي الخدمة المدارة (Managed Sservice Providers – MSP's) القادرين على إدارة البنية التحتية لتكنولوجيا المعلومات عن بُعد. اختر MSP المناسب الذي يقدم خدمة استباقية بناءً على احتياجات عملك.

- ابحث عن البساطة: إذا كنت شركة صغيرة ومتوسطة الحجم، فليس من الجيد اختيار الحلول المعقدة التي تتطلب تدريبًا مكلفًا وتأهيلًا لموظفيك. بدلاً من ذلك، ابحث عن حلول قياسية يسهل دمجها في قسم تكنولوجيا المعلومات الداخلي لديك.

4. كيفية اختيار مكونات البنية التحتية المناسبة Choosing the right infrastructure

تهدف قائمة مراجعة تكنولوجيا المعلومات هذه إلى سرد مشكلات تكنولوجيا المعلومات التي ستواجهها، ربما بشكل متكرر. يضمن كل عنصر في قائمة التحقق هذه وضوح متطلباتك بالإضافة إلى الإجراءات المطلوبة. بينما نقدم نظرة عامة فقط هنا، فإن قائمة المراجعة نفسها تقدم مزيدًا من التفاصيل، حيث يتم سرد جميع العناصر كما يلي:

ضع خطة تصميم المكتب

يجب تحديد موقع كل قسم وعدد محطات العمل، وغرفة خادم، وغرفة اجتماعات، وطابعات، وآلات تصوير، ومعدات شبكة WiFi

تحديد مزود خدمة الإنترنت

اختر مزود خدمة الإنترنت بالإضافة إلى مزود خدمة إنترنت مساند (احتياطي) وتفاوض على أفضل حزمة تخدم احتياجات ونطاق أعمال شركتك.

ترتيب أولويات الإعداد

يعتبر قسم تكنولوجيا المعلومات من الأقسام المهمة لأي عملية تجارية. من خلال الترتيب لإكمال إعداد تكنولوجيا المعلومات أولاً، ستضمن أن شركتك ستعمل بسرعة. فيما يلي قائمة التحقق من الأولوية:

- غرفة الخادم
- البنية الأساسية للشبكة
- أجهزة التوجيه ونقاط الوصول (نقطة الوصول)
- محطات العمل
- UPS (مصدر طاقة احتياطي غير منقطع)
- الطابعات والماسحات الضوئية
- غرفة ا الاجتماعات

البنية التحتية لتكنولوجيا المعلومات

في الأعمال التجارية الصغيرة، من المغري جدًا شراء معدات جديدة دون حتى التفكير في كيفية تركيبها. تقع الشركات الصغيرة أيضًا في خطأ شراء المعدات في مكاتبها بناءً على تجربتها مع معدات "مماثلة" في منازلها. فشلوا في إدراك أن معظم المعدات المناسبة للاستخدام المنزلي لن تعمل بشكل جيد في بيئة الأعمال.

يجب عليك التأكد من أن المعدات التي تشتريها مناسبة لبيئة الأعمال.

بعض عناصر قائمة مراجعة البنية التحتية لتكنولوجيا المعلومات التي يجب مراعاتها:

- تأكد من التوافق مع الأجهزة الأخرى التي تستخدمها للتثبيت، إذا لم يكن لديك خبير في تكنولوجيا المعلومات داخليًا فاحصل على مساعدة احترافية.
- ضمان عقود كفالة وخدمة الأجهزة المناسبة.
- تأكد من وجود نظام تشغيل مشترك لتوحيد استكشاف الأخطاء وإصلاحها والصيانة.
- قم دائمًا بتثبيت أحدث برامج التشغيل الاصلية.

البرامج

تراخيص البرمجيات هي أصول قيمة لشركتك. من السهل تثبيت البرامج على جهاز الكمبيوتر وتنسى تمامًا أنها موجودة. من الأسهل نسيان ما إذا كان لديك عقد خدمة، وما يتضمنه، وما إذا كان عليك تجديده، ومتى.

تخيل نسيان تجديد اسم المجال الخاص بك! نعم، يحدث هذا على الرغم من تلقي العديد من رسائل البريد الإلكتروني، والتي تضيع في ظروف غامضة في بريدك الوارد. على الرغم من أن أسماء النطاقات رخيصة، إلا أنها لا تقدر بثمن كهوية لعملك.

لذلك، يجب عليك توحيد عمليات الشراء والترخيص والتجديد والتحديث. يجب أن يكون هناك شخص مسؤول عن ذلك ويجب توثيق كل شيء والوصول إليه بسهولة عند الحاجة.

بعض عناصر قائمة التحقق التي يجب وضعها في الاعتبار:

- تخصيص البرامج لتناسب احتياجات العمل
- التنزيل والتثبيت من قبل المستخدمين
- استخدم Mobile Device Management - MDM (إدارة الأجهزة المحمولة) لتقييم ونشر تحديثات الأمان لضمان تأمين الأجهزة المحمولة وأنظمة التشغيل والتطبيقات

تذكر. ان استخدام البرامج الغير مرخصة قد يتسبب في عبئ زائد على المعالج وتلف البيانات

السحابة

تقدم السحابة حلاً ممتازًا للشركات الصغيرة مما يسمح لها بتوسيع نطاق بنيتها التحتية ومواكبة أعمالها المتنامية. تعد السحابة مثالية للشركات الصغيرة لأنها ميسورة التكلفة وسريعة ومرنة. ومع ذلك قبل أن تتمكن من نقل عملك إلى السحابة، عليك التفكير في بعض الأسئلة المهمة.

بعض عناصر قائمة التحقق السحابية التي يجب مراعاتها:

- هل استخدامي للسحابة يتماشى مع التشريعات التنظيمية
- هل تلبي الخدمة السحابية متطلبات خصوصية البيانات والامتثال؟
- ما هو مستوى الخدمة الذي يمكن أن توفره السحابة لأعمالي
- تأكد من أن اتفاقية مستوى الخدمة (SLA) تتضمن بنودًا بشأن أوقات الاستجابة واستمرارية الأعمال والتعافي من الكوارث.
- من المسؤول عن تحديثات البرامج
- من لديه حق الوصول إلى البيانات

الأمن السيبراني_Cyber Security

من المرجح أن تقع الشركات الصغيرة في عادات سيئة تتعلق بلأمن السيبراني أكثر من الشركات الكبيرة. هذا لأن الشركات الصغيرة نادراً ما يكون لديها سياسة أو برمجيات قوية لأمن تكنولوجيا المعلومات في البداية. مع اعتماد كل تقنية جديدة، تزداد الحاجة إلى يقظة الأمن السيبراني. تحتاج الشركات الصغيرة إلى توخي المزيد من اليقظة لأن 43٪ من الهجمات الإلكترونية تستهدف الشركات الصغيرة.

بعض عناصر قائمة التحقق الخاصة بأمان تكنولوجيا المعلومات التي يجب مراعاتها:

- استخدم أفضل الممارسات لأمان كلمة المرور
- تقييد الوصول إلى النظام
- إدخال وإخراج المستخدم
- الأذونات وكلمات المرور وغيرها من قواعد السلامة والأمان والقواعد الإدارية
- المجلدات المشتركة ومنح / تقليل حقوق الوصول إلى البيانات والأنظمة والتطبيقات
- إدارة قواعد البيانات والوصول إليها
- شبكة WiFi وأجهزة آمنة
- إدارة استخدام الUSB ومحركات أقراص صلبة خارجية
- سياسة احتواء وتنظيف وصيانة الأجهزة المصابة والمعطلة
- أمن معدات وموجودات تكنولوجيا المعلومات
- إدارة الشبكة الخاصة الافتراضية Virtual Private Network - VPN
- استخدم نسخ البرامج الأصلية المرخصة
- سياسات االستخدام الأجهزة والانترنت
- سياسة تحديث البرمجيات والتطبيقات
- التعافي من الكوارث
- التدريب وورش العمل

5. سياسات إدارة البنية التحتية Infrastructure Policies

فيما يلي مجموعة من السياسات التي يجب اتباعها عند التعامل مع مكونات البنية التحتية من معدات وبرمجيات:

- يتوجب على الموظفين استخدام الأصول (الأجهزة) بعناية ومهنية واحتراف.
- في حال حدوث اي مشكلة في اي جهاز لتكنولوجيا المعلومات، يجب الإتصل مباشرة بالفني المختص.
- على الموظفين عدم العبث بالأسلاك الكهربائية او كابلات الشبكة الموصلة بالأجهزة والمعدات
- يجب تغيير كلمات السر بصورة آلية (تلقائيا) على اساس شهري زيادة في مستوى الأمان.
- يجب ان تبدأ كلمة السر بأحرف أبجدية، تتضمن ارقام او أحرف فقط، وتتكون من ستة (6) أحرف على الأقل.
- يجب ان لا يسمح النظام بتكرار استخدام نفس كلمات السر.
- يجب ان يكون لدى الموظفين المخولين باستخدام الانترنت، برنامج محدث مضاد للفيروسات (UPDATED antivirus program) لزيادة تأمين الشبكة وحمايتها.
- يمنع الموظفون المخولون باستخدام تاتنترنت من تصفح اي من المواقع المحجوبة.
- تصفح الانترنت لأغراض غير مرتبطة بالعمل يجب ان لا يتم خلال اوقات العمل الرسمية.
- يجب تعريف جدران الحماية (Firewall) بشكل صحيح ودقيق
- حصر خيارات الوصول الى الانترنت على الموظفين المخولين (المحددين) من قبل الإدارة.
- سوف يحظى مدير الشبكات ومشرف الشبكات بإمكانية الوصول عن بعد الى جميع الحواسيب الثابته والنقالة لأسباب تتعلق بالمراجعة والتدقيق والصيانة والتحديثات ان استدعي ذالك
- يجب إثارة موضوع تأمين وحماية البيانات عند ترك اي موظف للعمل.
- يجب على الموظفين تخزين المعلومات والبيانات الخاصة بالعمل على السحبة قبل مغادره المكتب، وبالذات على الحواسيب النقالة كونها عرضه للضياع او السرقه بدرجة كبيرة.
- يجب منع استخدام جميع الاقراص المدمجه والمرنة و USB من قبل الموظفين في الشركه وعلى جميع أجهزة المؤسسة كإجراء أمني الا اذا كان مصرح لهم وذالك للحماية ضد الفيروسات والمتطفلين والمخربين.
- إن الطابعات والماسحات الضوئية وأجهزة نقاط الإستخدام اللاسلكي .... الخ؛ جميعها ملك للشركة وبناء على ذلك لا يجوز استخدامها مطلقا لأسباب شخصية.

- يجب العمل على تركيب برنامج مضاد للفيروسات مرخص، محدث، وفعال في كل حاسوب ثابت او نقال وفي جميع الخوادم ويجب تحديثه يوميا.

- في حال عدم تمكن الفني المسؤول من معالجة او حل مشكلة في جهاز معين (مثل تعطل جهاز الحاسوب، الطابعة، الماسحة الضوئية...الخ) ويتطلب الأمر صيانة الجهاز خارج مقر الشركة؛ يجب الحصول على موافقة الإدارة بذلك. يقوم الفني المعني بتسليم الجهاز الى ممثل شركة الصيانة وتوقيعه على الإستلام بعد أخذ تصريح بذلك من مدير تكنولوجيا المعلومات؛ وبعد إزالة اية معلومات سرية من ذاكرة الجهاز.

- على المستخدمين الإمتناع عن إعطاء كلمة السر الخاصة بهم الى اي شخص داخل وخارج الشركة. كما ينبغي عليهم عدم كتابة كلمة السر في اي مكان كإجراء احتياطي لزيادة مستوى الأمان.

- في حال اضطرار دائرة تكنولوجيا المعلومات لاستبدال كلمة السر نتيجة لفقدها من قبل المستخدم، يجب على مشرف الشبكة تغيير كلمة السر من المصدر الأساسي وإبلاغ المستخدم بكلمة السر الجديدة.

تذكر. راجع دليل سياسات وإجراءات المشتريات ضمن منصة جروث بايتس لشراء المعدات والبرمجيات والأصول المتعلقة بالبنية التحتية لتقنية المعلومات، بالإضافة إلى دليل سياسات وإجراءات الأصول الثابتة للحفاظ عليها ومتابعتها وتحديد معدلات الاستخدام.

6. التخزين والنسخ الاحتياطي واسترجاع البيانات Storage, Backup and Recovery of Data

الهدف من وضع سياسة معالجة الكوارث في تكنولوجيا المعلومات وسياسة البيانات الإحتياطية هو لتوفير الإستمرارية واستعادة البيانات والأنظمة الحساسة.

ينبغي التأكد من اجراء النسخ الإحتياطي (Backup) للبيانات الحساسة دوريا وحفظ النسخ المستخرجة في موقع بعيد عن الأنظار. كما يجب وضع خطة عمل محددة للحفاظ على الأصول الحساسة فيما يتعلق بالإجراءات المتكررة لتنفيذ عملية النسخ الإحتياطي (Backup)، بالإضافة الى إجراءات معالجة والنجاة من الكوارث سواء المسببة بفعل عوامل بشرية او خارجية.

الجزء المتعلق بالنسخ الإحتياطي (التخزين) للبيانات في هذه السياسة ينطبق على جميع أقسام الشركة بالاضافة الى اي أطراف ثالثة التي تستخدم معدات وأجهزة متصلة مع شبكة الشركة او التي تقوم بمعالجة او تخزين البيانات الحساسة المملوكة للشركة.

من المهم تدريب موظفو الشركة على إعداد اجراءات نسخ احتياطية للبيانات المتوفرة على انظمة تكنولوجيا المعلومات الموكلة إليهم.

وينطبق الجزء المتعلق بمعالجة والخروج من وضع كارثي في هذه السياسة على جميع مدراء الشبكات، مدراء الأنظمة، ومدراء التطبيقات، وهم المسؤولون عن الأنظمة الحساسة او تحصيل وتجميع البيانات الحساسة المتوفرة تلقائيا على المزود الخاص بهم او على القرص الصلب (hard disk) لجهاز الحاسوب.

مشرف الشبكة هو المسؤول عن النسخ الإحتياطي (تخزين) للبيانات المحفوظة في الأنظمة المركزية وقواعد البيانات ذات العلاقة. بينما تقع عملية النسخ الإحتياطي (تخزين) للبيانات الموجودة على وحدات (اجهزة) العمل الفردية للموظفين على عاتق المستخدم، سواء كان الجهاز مملوكا للموظف او للشركة.

على جميع اجراءات النسخ (التخزين) الإحتياطي أن تتوافق مع أفضل الممارسات والإجراءات ويمكن تحديدها من خلال الخطوات التالية:

- جميع البيانات ونظم التشغيل واستخدام ملفات يجب ان تدعم بالصيانة والتحديثات بشكل منتظم.
- يجب انشاء والمحافظة على سجلات توضح طبيعة المواد التي تم حفظها (تخزينها) وأمكان حفظها
- يجب حفظ (تخزين) السجلات الخاصة بترخيص البرمجيات
- يتوجب وضع بطاقات تعريفية على المواد المحفوظة (المخزنة) والإحتفاظ بسجلات دقيقة بعمليات النسخ الإحتياطي (التخزين) وتحديد المجموعة التي تنتمي اليها المواد المخزنة.
- ينبغي تخزين نسخ من البيانات المخزنة، بالإضافة الى سجل المواد المحفوظة، في مكان بعيد عن الأنظار، وعلى مسافة لتجنب الأضرار في حال وقوع كارثة في الموقع الرئيسي.
- يتوجب اجراء تجارب متكررة على استعاده البيانات / البرمجيات من النسخ الاحتياطية، لضمان امكانية الاعتماد على استخدامها في الحالات الطارئة.

يتم حفظ (النسخ الإحتياطية) لجميع الرسائل الإلكترونية وملفات الشبكات بانتظام باستخدام اجهزة الحفظ (الدعم الإحتياطي)، ويتم حفظ (نسخ) الملفات بشكل كامل اسبوعيا وحفظ (نسخ) البيانات المهمة يوميا. ويتم تخزين الملفات المحفوظة على الخادم (server) أو نظم التخزين السحابية.

عند فقدان أو ضياع البيانات، يمكن للمستخدم الاتصال بمشرف و/او مدير الشبكه من خلال ارسال طلب استعاده (استرجاع) البيانات موضحا ماهية البيانات والمطلوبة ووقت فقدان هذه البيانات.

7. سياسات الدعم التقني Technical Support Policies

يجب إرسال جميع طلبات الدعم من خلال البريد الإلكتروني أو عن طريق الاتصال الهاتفي أو إن كان هناك نظام مستخدم للدعم فيجب استعماله.

من المهم أن تتضمن طلبات الدعم جميع المعلومات المطلوبة والشرح الكافي للمشكلة وأي مستندات داعمة. بمجرد تقديم طلب للدعم، سيتم توجيههُ تلقائيًا إلى مجموعة التذاكر Ticketing System.

المطلوب من ممثل الدعم الفني الرد ضمن إطار زمني على هذا الطلب وضمن سياسة مستوى الخدمة Service Level وهو مسؤول عن ضمان الحلول الدقيقة وخطوات استكشاف الأخطاء وإصلاحها.

الممثل مسؤول أيضًا عن عمر التذكرة حتى يتم حل المشكلة أو ما يلزم من تصعيد التذكرة إلى شخص آخر. سيتم تحديث حالة التذكرة بعد كل متابعة مع الموظف وسيتم إدخال ملاحظات مفصلة عن التذكرة قبل وضع التذكرة في حالة الإغلاق.

مستويات الشدة وأهداف مستوى الخدمة

اعتمادًا على شدة المشكلة، يتم تحديد أهدافًا لمستوى الخدمة لحل المشكلة وهي كما يلي:

المستوى 1 - عاجل

- التأكيد التلقائي للتذكرة
- 2 ساعة استجابة أولية
- 24 ساعة الوقت لاقصى للوصول الى قرار

المستوى 2 - مرتفع

- التأكيد التلقائي للتذكرة
- 4 ساعات استجابة أولية
- 48 ساعة الوقت لاقصى للوصول الى قرار

المستوى 3 - متوسط

- التأكيد التلقائي للتذكرة
- 8 ساعات استجابة أولية
- 72 ساعة الوقت لاقصى للوصول الى قرار

المستوى 4 - منخفض

- التأكيد التلقائي للتذكرة
- 8 ساعات استجابة أولية
- 72 ساعة الوقت لاقصى للوصول الى قرار

تعريفات مستويات الخطورة

المستوى 1 - عاجل

هي مشكلة إنتاج كارثية قد تؤثر بشدة على الأنظمة الخاصة بالموظف، أو حيث تكون الأنظمة معطلة أو لا تعمل؛ او هناك فقدان للبيانات ولا يوجد حل إجرائي موجود.

المستوى 2 - مرتفع

المشكلة خطيرة، حيث يعمل نظام الموظف ولكن بقدرة منخفضة للغاية. يتسبب الوضع في إحداث تأثير كبير على أجزاء من العمليات التجارية والإنتاجية للعميل. يتعرض النظام لاحتمال فقدان أو انقطاع الخدمة.

المستوى 3 - متوسط

المشكلة متوسطة الخطورة ذات تأثير متوسط إلى منخفض تتضمن فقدًا وظيفيًا جزئيًا غير حرج. يضعف الموقف بعض العمليات، لكنه يسمح للموظف بمواصلة العمل.

المستوى 4- منخفض

وهي ملاحظة مخصصة للاستخدام العام أو توصيات لمنتج مستقبلي أو تحسين أو تعديل دون وجود أي تأثير على جودة الأنظمةأو أدائها أو وظائفها.

عملية تصعيد المشكلات داخل القسم التقني

أثناء إرسال طلبات المشاكل التقنية من الموظفين، تتم مراجعتها تلقائيًا بواسطة فنيي دعم خبير من المستوى 1. يجب أن يكون فني الدعم من المستوى 1 قادرًا على مساعدة العميل في حل المشكلة. في حالة الحاجة إلى موارد وخبرات إضافية، سيتم استشارة هذه الموارد على النحو التالي:

- تعيين المستوى 1 - فني دعم معين في البداية والذي سيعمل مع المستخدم لمحاولة حل المشكلة.
- تعيين المستوى 2 - إذا قرر فني الدعم من المستوى 1 أن هناك حاجة إلى خبرة إضافية أو أن استشاري الدعم غير قادر على حل المشكلة خلال وقت الحل المستهدف، فسيتم تصعيد الحالة إلى موارد المستوى 2 ذات الخبرة المتخصصة لحل الحالة.

- تعيين المستوى 3 - إذا كان أخصائي المستوى 2 غير قادر على حل المشكلة خلال فترة زمنية معقولة، فسيتم نقل الحالة إلى أحد كبار أعضاء فريق تطوير المنتج للحصول على المساعدة.

ساعات الدعم

يتم تقديم الدعم ضمن ساعات العمل القياسية هي من 9:00 صباحًا إلى 5:00 مساءً باستثناء أيام العطلات. مع الاخذ بعين الاعتبار بأن أوقات توفر الدعم تختلف من شركة الى أخرى حسب احتيجات موظفيها وعملائها.

8. مؤشرات أداء البنية التحتية IT Infrastruture KPI's

المؤشرات الرئيسية التي يجب النظر إليها لتحديد فيما إذا كان فريق البنية التحتية ضمن تقنية المعلومات يعمل بالكفاءة المطلوبة هي كما يلي:

- إجمالي تذاكر الدعم التقني المغلقة مقابل التذاكر المفتوحة
- تسليم مشاريع البنية التحتية ضمن حدود الميزانية والمواعيد
- الميزات الجديدة المطورة: كم عدد الميزات التي يتم تطويرها باستمرار؟
- عدد الأخطاء الحرجة: كم عدد الأخطاء التي تحدث بانتظام؟
- تعطل الخادم: لماذا ومتى يحدث التوقف؟
- متوسط الوقت للإصلاح: ما مدى كفاءة التعامل مع الأحداث غير المتوقعة؟
- عدد التذاكر التي لم يتم حلها لكل موظف
- نسبة إعادة فتح التذاكر المغلقة مسبقاً
- نسبة موظفو دعم تكنولوجيا المعلومات لكل مستخدم: هل هناك ما يكفي من دعم تكنولوجيا المعلومات؟
- دقة تقديرات الوقت اللازم لإغلاق تذكرة