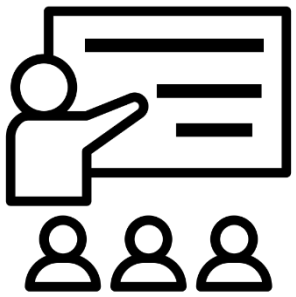
GROWTH BYTES

دليل سياسات

الدعم التقني – IT Technical Support

قطاع صيانة السيارات والمعدات الثقيلة



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.

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

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.