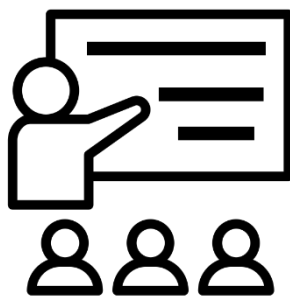


دليل سياسات

الدعم التقني – IT Technical Support قطاع المقاولات



قائمة المحتويات

3IT TECHNICAL SUPPORT الدعم التقني
3المقدمة والمبادئ العامة
4IT INFRASTRUCTURE COMPONENTS أجزاء البنية التحتية لإدارة تكنولوجيا المعلومات
6IT INFRASTRUCTURE COMPONENTS مكونات البنية التحتية
8CHOOSING THE RIGHT INFRASTRUCTURE كيفية اختيار مكونات البنية التحتية المناسبة
11INFRASTRUCTURE POLICIES سياسات إدارة البنية التحتية
12STORAGE, BACKUP AND RECOVERY OF DATA التخزين والنسخ الاحتياطي واسترجاع البيانات
13TECHNICAL SUPPORT POLICIES سياسات الدعم التقني
16IT INFRASTRUTURE KPI'S مؤشرات أداء البنية التحتية

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 ذلك.

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 مسؤولان 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 أيضًا أمن الشبكات، مثل كشف أي تسلل خارجي والوقاية منه، ومعلومات الأمان وإدارة كافة الأحداث المتعلقة بتلك الأنظمة، وكذلك تدرج 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 المعلومات:

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 ملاءمة 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 تتضمن 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 وتفصيل مُزويديها وأرشفة سجلاتها.

أداء الشبكة

يعد أداء الشبكة أمرًا بالغ الأهمية لعملياتها 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

أُثمن 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.

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 كفاءة 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 عبء زائد على المعالج وتلف البيانات

السحابة

تقدم السحابة حلاً ممتازاً 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 تليي الخدمة السحابية متطلبات خصوصية البيانات والامتثال؟
- ما هو مستوى الخدمة الذي يمكن أن توفره السحابة لأعمالي
- تأكد من أن اتفاقية مستوى الخدمة (SLA) تتضمن بنوداً 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 بالأمن 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 توشي 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 الـ USB ومحركات أقراص صلبة خارجية
- سياسة احتواء وتنظيف وصيانة الأجهزة المصابة والمعلقة
- أمن معدات وموجودات تكنولوجيا المعلومات
- إدارة الشبكة الخاصة الافتراضية Virtual Private Network - VPN
- استخدم نسخ البرامج الأصلية المرخصة
- سياسات استخدام الأجهزة والانترنت
- سياسة تحديث البرمجيات والتطبيقات
- التعافي من الكوارث
- التدريب وورش العمل

- 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 لفقدانها 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 بالإضافة 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 إعدادات نسخ احتياطية للبيانات المتوفرة على أنظمة 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.