**وب**

* مستندات مربوط به كنترل مركزي وب مانند روترها، پروكسي و فايروال
* مستندات مربوط به افراد تعيين كننده كنترل
* افرادي كه مي توانند از وب استفاده كنند
* سايت هايي كه كاربران به آن دسترسي پيدا مي كنند
* زمان استفاده از سايت هاي مذكور
* سيستم هاي كنترل محتوايي صفحات وب و مدت زمان مجاز دسترسي
* مستندات مربوط به گزارش هاي كاربران، صفحات ديده شده توسط آنان و افرادي كه اين گزارش ها را دريافت مي كنند و فاصله زماني گزارش ها
* مستندات مربوط به مقررات برخورد با كاربران سايت هاي غيرمجاز
* ثبت كليه فعاليت هاي وب همراه با نام كاربران
* اطمينان اينكه كليه كاربران از مقررات امنيتي مربوط به اينترنت مطلع اند،
* پياده سازي GPO جهت موارد ايمني (مانند اكتيو ايكس هاي غير مجاز) در اينترنت
* استفاده از نرم افزار امنيت دانلود و پيشگيري از نفوذ برنامه هاي مزاحم و همچنين پيشگيري از استفاده بي مورد دانلودهاي صوتي – تصويري

**نام كاربري و كلمه رمز**

* پياده سازي كلمه رمز پيچيده، الزام به تغيير رمز هر چند ماه يك بار، ممنوعيت استفاده از كلمه رمز تكراري و مسدود كردن كاربر به هنگام ورود چند باره ناموفق
* ثبت ورود موفق و ناموفق به خصوص در مورد كاربران مدير
* تغيير نام كاربر پيش فرض مدير administrator، root و ...
* استفاده از سيستم Single-Sign-on=sso جهت استفاده از يك نام كاربري و رمز در برنامه هاي متعدد
* مستندسازي سيستم نام كاربري و رمز و آموزش آن به كاربران
* انجام عمليات شكستن رمز كاربر مدير به صورت دوره اي جهت بررسي امنيت و قوي بودن رمز آن

**چت آنلاين**

* مسدود كردن كليه چت آنلاين به جز موارد كاملاً ضروري
* در صورت لازم بودن چت در برخي موراد، بايد از برنامه اي كه استفاده از اين امكان را كنترل مي نمايد و تمامي مكالمات را ذخيره مي كند استفاده نمود.
* مستند سازي مقررات چت و آموزش آن به كاربران

**ايميل**

* مستند سازي ميزان ذخيره سازي ايميل توسط هر كاربر
* كنترل دسترسي بيروني به گروه هاي داخلي كاربران
* كنترل محتوايي نامه ها جهت جلوگيري از خروج اطلاعات محرمانه
* استفاده از برنامه ضد هرزنامه
* آموزش به كاربران جهت استفاده درست از ايميل، خودداري از دادن آدرس ايميل به سايت ها و مراكز ناشناس و آموزش مقابله با هرزنامه هاي دريافتي
* برنامه ضد ويروس ايميل
* استفاده از برنامه آرشيو ايميل جهت بازيابي اضطراري و كنترل حجم بانك اطلاعاتي ايميل
* تدوين مقررات استفاده شخصي از ايميل سازماني و آموزش آن به كاربران
* آموزش در مورد phishing

**مجوز دسترسي فايل ها**

* مستندسازي مالكان فايل هاي حساس. اين افراد مشخص خواهند كرد كه كدام كاربر به چه فايل هايي دسترسي دارد. البته در نهايت بايد سيستم عامل يا نرم افزار مورد استفاده نيز علاوه بر كاربر مشخص گردد.
* نظارت بر پوشه هاي اشتراكي با مجوز everyone
* ثبت گزارش هاي دسترسي موفق و ناموفق به فايل ها و تغيير آنها.

**پشتيبان گيري**

* مشخص نمودن اينكه چه داده هايي در چه فاصله زماني بايد پشتيبان گيري شوند و چه مدت نگهداري گردند.
* مستند سازي اينكه چند وقت يك بار آزمايش امكان تيمي بازيابي فايل هاي پشتيبان صورت گيرد.
* رمز نگاري اطلاعات پشتيبان در نوارها جهت پيشگيري از سرقت اطلاعات
* اطمينان از اينكه فايل هاي پشتيبان در خارج از سايت هم نگهداري مي شوند و مستند سازي روش اجرايي

**امنيت فيزيكي**

* مستندسازي موارد امنيت فيزيكي
* قفل بودن در اتاق هاي سرور، قفل هاي الكترونيكي با امكان ثبت ورود و خروج افراد
* نداشتن پنجره هاي قابل شكستن در اتاق ها
* آيا Usp يا موارد برق موجود است؟
* سيستم هاي هشدار و كنترل و اطفا حريق وجود دارند؟
* دوربين هاي مدار بسته
* امنيت فيزيكي دسترسي به كنسول ها و ترمينال هايي كه به سرور ها، سوئيچ ها و روتر ها وصل مي شوند.

**مديريت بحران**

* مستندسازي روش مديريت بحران. روش مذكور بايد حاوي حالت هاي مربوط به حوادث طبيعي نيز باشد.

**كامپيوترهاي دسكتاپ و لپ تاپ**

* مستندات مربوط به كنترل دسكتاپ ها و لپ تاپ ها
* كاربران اختيارات مديريتي روي كامپيوتر خود ندارند مگر در صورت نياز خاص يك نرم افزار كاربران اجازه ورود به صورت محلي به سيستم را ندارند و الزاما بايد از طريق Domain وارد شوند.
* استفاده از رمزنگاري جهت پيشگيري از انتشار غير مجاز اطلاعات به هنگام گم شدن يا سرقت كامپيوترها
* استفاده از ضد ويروس و ضد جاسوس در همه كامپيوترها
* استفاده از فايروال در لپ تاپ ها چون معمولاً از يك شبكه به شبكه ديگري مي روند.
* استفاده از GPO جهت محدود كردن كاربران (مثلاً در مورد نصب برنامه ها)
* تدوين روش اجرايي جهت حصول اطمينان از نصب آخرين به روزرساني امنيتي
* اعمال امنيت بر حافظه هاي فلش (USB)

**دسترسي از راه دور**

* كنترل كاربراني كه مجوز دسترسي تلفني يا VPN دارند
* مستندسازي مقررات دسترسي از راه دور
* ثبت ورود موفق يا ناموفق از راه دور
* آزمايش دوره اي امنيت دسترسي راه دور از بيرون سازمان
* پياده سازي روشي جهت اطمينان از به روز بودن سيستم ها ي متصل شونده و ضد ويروس آنها براي جلوگيري از نفوذ ويروس به سيستم هاي سازمان
* استفاده از روش ثانويه شناسايي كاربر در دسترسي راه دور جهت پيشگيري از نفوذ از طريق سرقت كلمه رمز

**سرورها- روترها- سوئيچ ها**

* اجراي ضدويروس و ضد جاسوس در سرورها
* اطمينان از آخرين به روز رساني ها
* ثبت وقايع اين دستگاه ها به سرور وLog مركزي
* اجراي برنامه نظارت بر كارآيي سيستم ها جهت هشدار موارد غيرعادي
* مستند سازي كاربراني كه دسترسي مديريتي به اين سيستم ها دارند.
* مستند سازي روش دسترسي و سطوح دسترسي داده شده به تأمين كنندگان كه جهت پشتيباني يا تغيير در سيستم نياز به دسترسي دارند.
* مستند سازي موارد امنيت مربوط به توليد و محيط آزمايش نرم افزارها

**شبكه اينترنت/ شبكه خارج از سازمان**

* آزمايش دوره اي نفوذ بر روي اتصالات اينترنت
* استفاده از فايروال و ثبت آنچه فايروال از آن ممانعت مي نمايد
* مستندسازي فايروال و قوانين آن
* تدوين سيستم مقابله با ورود غيرمجاز كه از فايروال نيز عبور كرده باشد.
* حداقل نگهداشتن تعداد اتصالات اينترنت
* ايجاد سيستم مديريت اطلاعات امنيتي سازمان

**بي سيم**

* آزمايش دوره اي نفوذ از بيرون به شبكه هاي بي سيم
* استفاده از قوي ترين رمزنگاري WEP موجود و ممكن
* استفاده از تجهيزات امنيت بي سيم كه از انتشار امواج شبكه هاي بيسيم به بيرون از محدوده سازمان پيشگيري كند.
* استفاده از شناسايي كاربران بي سيم بر مبناي 802.1x علاوه بر سيستم عامل
* الزام كاربران به اتصال VPN به شبكه بي سيم
* مستند سازي مقررات بي سيم و آموزش آن به كاربران

**ثبت وقايع**

* استفاده از سيم مركزي ثبت گزارش
* مستندسازي روش ثبت گزارش ها، كاربراني كه مجاز به ديدن آن هستند مدت زمان نگهداري گزارش و هر آنچه علاوه بر اينها بايد ثبت گردد.
* دستگاه هاي PDA و موبايل
* مستند سازي استفاده هاي درست و نادرست از موبايل و PDA
* استفاده از دستگاه ها و امكاناتي كه از راه دور PDA يا موبايل را از بين برده اطلاعات آن را غير قابل بازيابي كنند.
* مستند سازي انواع موبايل هايي كه پشتيباني مي شوند.

**مستندسازي و مديريت تغييرات**

* مستند سازي اينكه چه كسي تغييرات قوانين امنيتي را كنترل و چه كسي آنها را به روز خواهد كرد.
* مستند سازي فرآيند گردش و ثبت قبل از اعمال آنها.