وب

- ☐ مستندات مربوط به کنترل مرکزی وب مانند روترها، پروکسی و فایروال
- ☐ مستندات مربوط به افراد تعیین کننده کنترل
- ☐ افرادی که می توانند از وب استفاده کنند
- ☐ سایت هایی که کاربران به آن دسترسی پیدا می کنند
- ☐ زمان استفاده از سایت های مذکور
- ☐ سیستم های کنترل محتوایی صفحات وب و مدت زمان مجاز دسترسی
- ☐ مستندات مربوط به گزارش های کاربران، صفحات دیده شده توسط آنان و افرادی که این گزارش ها را دریافت می کنند و فاصله زمانی گزارش ها
- ☐ مستندات مربوط به مقررات برخورد با کاربران سایت های غیرمجاز
- ☐ ثبت کلیه فعالیت های وب همراه با نام کاربران
- ☐ اطمینان اینکه کلیه کاربران از مقررات امنیتی مربوط به اینترنت مطلع اند،
- ☐ پیاده سازی GPO جهت موارد ایمنی (مانند اکتیو ایکس های غیر مجاز) در اینترنت
- ☐ استفاده از نرم افزار امنیت دانلود و پیشگیری از نفوذ برنامه های مزاحم و همچنین پیشگیری از استفاده بی مورد دانلودهای صوتی – تصویری

نام کاربری و کلمه رمز

- ☐ پیاده سازی کلمه رمز پیچیده، الزام به تغییر رمز هر چند ماه یک بار، ممنوعیت استفاده از کلمه رمز تکراری و مسدود کردن کاربر به هنگام ورود چند باره ناموفق
- ☐ ثبت ورود موفق و ناموفق به خصوص در مورد کاربران مدیر
- ☐ تغییر نام کاربر پیش فرض مدیر administrator، root و ...
- ☐ استفاده از سیستم Single-Sign-on=sso جهت استفاده از یک نام کاربری و رمز در برنامه های متعدد
- ☐ مستندسازی سیستم نام کاربری و رمز و آموزش آن به کاربران
- ☐ انجام عملیات شکستن رمز کاربر مدیر به صورت دوره ای جهت بررسی امنیت و قوی بودن رمز آن

چت آنلاین

- ☐ مسدود کردن کلیه چت آنلاین به جز موارد کاملاً ضروری
- ☐ در صورت لازم بودن چت در برخی موراد، باید از برنامه ای که استفاده از این امکان را کنترل می نماید و تمامی مکالمات را ذخیره می کند استفاده نمود.
- ☐ مستند سازی مقررات چت و آموزش آن به کاربران

ایمیل

- ☐ مستند سازی میزان ذخیره سازی ایمیل توسط هر کاربر
- ☐ کنترل دسترسی بیرونی به گروه های داخلی کاربران
- ☐ کنترل محتوایی نامه ها جهت جلوگیری از خروج اطلاعات محرمانه
- ☐ استفاده از برنامه ضد هرزنامه
- ☐ آموزش به کاربران جهت استفاده درست از ایمیل، خودداری از دادن آدرس ایمیل به سایت ها و مراکز ناشناس و آموزش مقابله با هرزنامه های دریافتی
- ☐ برنامه ضد ویروس ایمیل
- ☐ استفاده از برنامه آرشیو ایمیل جهت بازیابی اضطراری و کنترل حجم بانک اطلاعاتی ایمیل
- ☐ تدوین مقررات استفاده شخصی از ایمیل سازمانی و آموزش آن به کاربران
- ☐ آموزش در مورد phishing

مجوز دسترسی فایل ها

- ☐ مستندسازی مالکان فایل های حساس. این افراد مشخص خواهند کرد که کدام کاربر به چه فایل هایی دسترسی دارد. البته در نهایت باید سیستم عامل یا نرم افزار مورد استفاده نیز علاوه بر کاربر مشخص گردد.
- ☐ نظارت بر پوشه های اشتراکی با مجوز everyone
- ☐ ثبت گزارش های دسترسی موفق و ناموفق به فایل ها و تغییر آنها.

پشتیبان گیری

- ☐ مشخص نمودن اینکه چه داده هایی در چه فاصله زمانی باید پشتیبان گیری شوند و چه مدت نگهداری گردند.
- ☐ مستند سازی اینکه چند وقت یک بار آزمایش امکان تیمی بازیابی فایل های پشتیبان صورت گیرد.
- ☐ رمز نگاری اطلاعات پشتیبان در نوارها جهت پیشگیری از سرقت اطلاعات
- ☐ اطمینان از اینکه فایل های پشتیبان در خارج از سایت هم نگهداری می شوند و مستند سازی روش اجرایی

امنیت فیزیکی

- ☐ مستندسازی موارد امنیت فیزیکی
- ☐ قفل بودن در اتاق های سرور، قفل های الکترونیکی با امکان ثبت ورود و خروج افراد
- ☐ نداشتن پنجره های قابل شکستن در اتاق ها
- ☐ آیا Usp یا موارد برق موجود است؟
- ☐ سیستم های هشدار و کنترل و اطفا حریق وجود دارند؟
- ☐ دوربین های مدار بسته
- ☐ امنیت فیزیکی دسترسی به کنسول ها و ترمینال هایی که به سرور ها، سوئیچ ها و روتر ها وصل می شوند.

مدیریت بحران

- ☐ مستندسازی روش مدیریت بحران. روش مذکور باید حاوی حالت های مربوط به حوادث طبیعی نیز باشد.

کامپیوترهای دسکتاپ و لپ تاپ

- ☐ مستندات مربوط به کنترل دسکتاپ ها و لپ تاپ ها
- ☐ کاربران اختیارات مدیریتی روی کامپیوتر خود ندارند مگر در صورت نیاز خاص یک نرم افزار کاربران اجازه ورود به صورت محلی به سیستم را ندارند و الزاما باید از طریق Domain وارد شوند.
- ☐ استفاده از رمزنگاری جهت پیشگیری از انتشار غیر مجاز اطلاعات به هنگام گم شدن یا سرقت کامپیوترها
- ☐ استفاده از ضد ویروس و ضد جاسوس در همه کامپیوترها
- ☐ استفاده از فایروال در لپ تاپ ها چون معمولاً از یک شبکه به شبکه دیگری می روند.
- ☐ استفاده از GPO جهت محدود کردن کاربران (مثلاً در مورد نصب برنامه ها)
- ☐ تدوین روش اجرایی جهت حصول اطمینان از نصب آخرین به روزرسانی امنیتی
- ☐ اعمال امنیت بر حافظه های فلش (USB)

دسترسی از راه دور

- ☐ کنترل کاربرانی که مجوز دسترسی تلفنی یا VPN دارند
- ☐ مستندسازی مقررات دسترسی از راه دور
- ☐ ثبت ورود موفق یا ناموفق از راه دور
- ☐ آزمایش دوره ای امنیت دسترسی راه دور از بیرون سازمان
- ☐ پیاده سازی روشی جهت اطمینان از به روز بودن سیستم ها ی متصل شونده و ضد ویروس آنها برای جلوگیری از نفوذ ویروس به سیستم های سازمان
- ☐ استفاده از روش ثانویه شناسایی کاربر در دسترسی راه دور جهت پیشگیری از نفوذ از طریق سرقت کلمه رمز

سرورها- روترها- سوئیچ ها

- ☐ اجرای ضدویروس و ضد جاسوس در سرورها
- ☐ اطمینان از آخرین به روز رسانی ها
- ☐ ثبت وقایع این دستگاه ها به سرور وLog مرکزی
- ☐ اجرای برنامه نظارت بر کارآیی سیستم ها جهت هشدار موارد غیرعادی
- ☐ مستند سازی کاربرانی که دسترسی مدیریتی به این سیستم ها دارند.
- ☐ مستند سازی روش دسترسی و سطوح دسترسی داده شده به تأمین کنندگان که جهت پشتیبانی یا تغییر در سیستم نیاز به دسترسی دارند.
- ☐ مستند سازی موارد امنیت مربوط به تولید و محیط آزمایش نرم افزارها

شبکه اینترنت/ شبکه خارج از سازمان

- ☐ آزمایش دوره ای نفوذ بر روی اتصالات اینترنت
- ☐ استفاده از فایروال و ثبت آنچه فایروال از آن ممانعت می نماید
- ☐ مستندسازی فایروال و قوانین آن
- ☐ تدوین سیستم مقابله با ورود غیرمجاز که از فایروال نیز عبور کرده باشد.
- ☐ حداقل نگهداشتن تعداد اتصالات اینترنت
- ☐ ایجاد سیستم مدیریت اطلاعات امنیتی سازمان

بی سیم

- ☐ آزمایش دوره ای نفوذ از بیرون به شبکه های بی سیم
- ☐ استفاده از قوی ترین رمزنگاری WEP موجود و ممکن
- ☐ استفاده از تجهیزات امنیت بی سیم که از انتشار امواج شبکه های بیسیم به بیرون از محدوده سازمان پیشگیری کند.
- ☐ استفاده از شناسایی کاربران بی سیم بر مبنای 802.1x علاوه بر سیستم عامل
- ☐ الزام کاربران به اتصال VPN به شبکه بی سیم
- ☐ مستند سازی مقررات بی سیم و آموزش آن به کاربران

ثبت وقایع

- ☐ استفاده از سیم مرکزی ثبت گزارش
- ☐ مستندسازی روش ثبت گزارش ها، کاربرانی که مجاز به دیدن آن هستند مدت زمان نگهداری گزارش و هر آنچه علاوه بر اینها باید ثبت گردد.
- ☐ دستگاه های PDA و موبایل
- ☐ مستند سازی استفاده های درست و نادرست از موبایل و PDA
- ☐ استفاده از دستگاه ها و امکاناتی که از راه دور PDA یا موبایل را از بین برده اطلاعات آن را غیر قابل بازیابی کنند.
- ☐ مستند سازی انواع موبایل هایی که پشتیبانی می شوند.

مستندسازی و مدیریت تغییرات

- ☐ مستند سازی اینکه چه کسی تغییرات قوانین امنیتی را کنترل و چه کسی آنها را به روز خواهد کرد.
- ☐ مستند سازی فرآیند گردش و ثبت قبل از اعمال آنها.