ردیف	اقداماتی که باید انجام شود	روش اجرایی پیشنهادی	اقدامات انجام شده	مسئول انجام	طول زمان تقویتی اجرایی	نتیجه
۱	فراهم بودن و در صورت لزوم تهیه ابزارهای لازم و مورد اطمینان برای نگهداری نسخه های پشتیبان از اطلاعات ضروری					
۲	نسخه های پشتیبان باید حداقل در دو رسانه و در دومکان مجزا نگهداری شوند یکی از این مکان ها می بایست خارج از محیط فیزیکی کار باشد با توجه به اینکه دسترسی به آنها نباید زمان زیادی لازم داشته باشدOFISITE NACKUP					
۳	تمامی رسانه های قابل حمل ذخیره سازی (PORTABLE MEDIA)که برای نگهداری از نسخه های پشتیبان اطلاعات مورد استفاده قرار می گیرد باید در مکان مشخصی نگهداری شود و تنها این دستگاه ها حق دسترسی به این محدوده را داشته باشد					
۴	این رسانه ها حداقل ماهی یکبار مورد آزمایش بازیابی اطلاعات قرار گیرند و نتیجه این آزمایشها باید در فرم مربوطه ثبت گردد					
۵	لیستی از افراد، نرم افزار ها و پایگاه داده های که از اطلاعات آنها می بایست نسخه پشتیبان تهیه شود (تعیین دوره زمانی ، نوع اطلاعات و نوع نسخه پشتیبان ، مدت اعتبار نسخه های پشتیبان)					
۶	مشخص بودن مسیری جهت قراردادن اطلاعات توسط کاربران جهت تهیه نسخه پشتیبان از آنها و همچنین مشخص کردن زمان انجام این کار					
۷	از سرورها با درجه اهمیت بالا بطور کامل (سیستم عامل و اطلاعات داخل سیستم) نسخه پشتیبان تهیه گردد					

۸	مدت اعتبار نسخه های پشتیبان با توجه به نوع اطلاعات می بایست مشخص شود					
۹	تمام موارد امنیتی پیش آمده باید مستند شده (INCIDENT MANAGEMENT) و به اطلاع دبیر کمیته راهبری رسانده شود					
۱۰	بایستی تاریخ و زمان در کامپیوترها تنظیم و یکسان باشد و از تغییر دادن آنها توسط کاربران جلوگیری بعمل آید					
۱۱	استفاده از Password Policy مناسب در محیط ACTIVE DIRECTORY و دیگر سرویسهای سازمانی مانند سرویس E-MAIL ،سرویس پورتال و غیره					
۱۲	آموزشهای لازم جهت انتخاب PASSWORD مناسب توسط کاربر باید برای کاربران در نظر گرفته شود			سازمان		
۱۳	سخت افزارهایی (مانند سویچ ها) سرورها و یا سرویسها نباید دارای PASSWORD یکسان باشند					
۱۴	امکان REMEMBER MY PASSWORD نباید در هیچ صفحه احراز هویتی فعال باشد			سازمان		
۱۵	نگه داری از فایل رمزهای سرورها در مکان امن این فایل باید در اختیار مدیر واحد IT و مدیر شبکه باشد					
۱۶	ارسال Patch ها و Update ها به کامپیوترهای سرویس گیرنده (Client) نباید در ساعت های اوج کاری سازمان باشد .					
۱۷	قبل از نصب وصله های امنیتی ، سازگاربودن وصله های امنیتی با نرم افزارهای کاربردی سازمان باید در محیط تست مورد آزمایش قرار گیرند					
۱۸	ایجاد روال RollBack در صورت بروز خطا					
۱۹	LSUS SERVER باید دارای سخت افزار مناسب با این سرویس باشد . Linux Server Update Services					

۲۰	LSUS SERVER باید دارای اتصال امن دائم به اینترنت باشد Linux Server Update Services					
۲۱	روال مناسبی جهت نصب Patch و Update های مربوط به نرم افزارهای سازمانی باید تهیه شود					
۲۲	تدوین دستورالعمل بازیابی سیستم پس از ویروسی شدن آن و مشخص کردن مسئول انجام این امر					
۲۳	انجام آموزش های لازم برای کاربران جهت آشنایی با کارکرد آنتی ویروس در زمان اتصال رسانه های قابل جابجایی (Removable Media) به کامپیوتر					
۲۴	استفاده از آنتی ویروس معتبر برای سازمان دارای مدل سرویس دهی ، سرویس دهنده و سرویس گیرنده باشد					
۲۵	نسخه سرور آنتی ویروس باید دارای اتصال دائم بصورت امن با اینترنت باشد					
۲۶	بررسی Log ها و رخدادهای سرور آنتی ویروس در بازه های زمانی مشخص (حداقل ۷ روز)					
۲۷	سرورها با درجه اهمیت بالا باید روزانه توسط آنتی ویروس چک گردند . (غیر از زمان اوج ساعت کاری سازمان)					
۲۸	تنظیم نمودن آنتی ویروس به شکلی که در صورت آلوده شدن سیستم ها به ویروس بصورت خودکار مسئول سرویس آنتی ویروس را مطلع نماید .					
۲۹	در هنگام برقراری ارتباط بصورت مستقیم (Console) با تجهیزات شبکه (Swich Router...) میبایستی کلیه درگاه های مستقیم رمز عبوری داشته و پیشنهاد می گردد این رمز عبوری متفاوت بوده تا ضریب امنیت بیشتری را فراهم نماید.(مستند نمودن افرادی که به این تجهیزات دسترسی دارند و از رمز عبوری مطلع میباشند.)					

۳۳	الزام میباشد تا Administrator Account کلیه ایستگاه های کاری تغییر نام داده شده و غیر فعال گردد . این الزام در خصوص Domain Administration Account هم صادق است و میبایستی رمز عبور آن نیز در جای امن نگهداری شود ، همچنین برای انجام کارهای Administration در شبکه و ایستگاه های کاری از Delegation استفاده گردد و دسترسی ها با توجه به نیاز تعریف گردد و در غیر اینصورت برای سرویس های روزانه Administration پیشنهاد میگردد تا کاربری (Account) با توجه به آن سرویس تعریف و استفاده گردد					
۳۴	ثبت و مستند نمودن کلیه تغییرات و اتفاقات الزامی بوده و میبایستی این مستندات قابل پایش و طبقه بندی شده نیز باشند ، همچنین پیشنهاد میگردد از نرم افزارهای جانبی جهت بهبود سرویس Event Log Monitoring استفاده گردد و کلیه این مستندات میبایستی به مدت مشخص (توافق در کمیته راهبردی) نگهداری شوند . همچنین الزامی است که کلیه Event ها (بطور مثال Windows Event Viewer) توسط یک فرد مشخص و معین بصورت وتوالی مورد بازبینی و بررسی قرار گیرد					
۳۵	تمام رسانه ها باید در مکان مناسب که دارای قفل می باشد نگهداری شوند.				سازمان	
۳۶	استفاده از External Storage Media تنها با تصویب مدیر مربوط امکان پذیر می باشد .				سازمان	
۳۷	مدیران هر سرویس باید نوع دسترسی (... ، Delete ، Write ، Read) کاربران به سرویس همچنین اطلاعات مربوط را مشخص کنند				سازمان وشرکت	
۳۸	درخواست دسترسی کاربران باید توسط مدیر آن واحد مورد بررسی قرار گیرد					

۳۹	هر کاربر باید دارای یک Account یکتا برای یک سرویس باشد . کاربران نباید دارای Account دیگری باشد ، مگر در صورت نیاز و اجازه مدیر مربوطه					
۴۰	استفاده از User Account Delegation به جای استفاده از Administrator Account					
۴۱	بازنگری حقوق دسترسی ها در بازه های زمانی متناسب با اهمیت سرویس های مورد استفاده در سازمان مانند سرویس های ، Active Directory وEmail و Data Base					
۴۲	استفاده از امکانات Monitoring و ثبت وقایع جهت مشخص شدن Logon Failure					
۴۳	استفاده از Account Policy مناسب برای تمامی تجهیزات و سرویس ها جهت محدود کردن احتمال دسترسی غیر مجاز					
۴۴	در صورت استفاده از نرم افزارهای Tele Networking موارد امنیتی بالا در نظر گرفته شده باشد – استفاده از پروتکل SSH به جای Telnet – استفاده از امکان Session Time out – در صورت لزوم استفاده از امکان مشخص کردن محدودیت زمان برقراری ارتباط					
۴۵	در زمان تهیه یک سیستم جدید همواره وابستگی به دیگر تجهیزات و تخصص های لازم میبایست مورد توجه قرار گیرد تا از بروز هرگونه تهدید جدید که موجب به وجود آمدن یک ریسک شود جلوگیری به عمل آید					
۴۶	در صورت لزوم به ارسال فیزیکی اطلاعات مهم و یا رسانه های ذخیره سازی ، نوع بسته بندی باید به گونه ای باشد تا محرمانگی و سالم بودن آن تضمین گردد					
۴۷	ارسال اطلاعات باید توسط سرویس و یا افراد مطمئن انجام پذیرد و امکان پیگیری و رهگیری باید وجود داشته باشد .					

۴۸	استفاده از Labeling مناسب به گونه ای که مشان دهنده ء میزان اهمیت اطلاعات باشد					
۴۹	آموزش های لازم به کارکنان در خصوص امنیت ارتباطات باید ارایه شود .					
۵۰	قبل از پذیرش سیستم جدید باید تمامی موارد زیر مد نظر قرار گیرد : -بررسی قابلیت های پردازشی و ظرفیتی مورد نیاز برای سیستم جدید (منظور از سیستم جدید در این مورد تجهیزات کامپیوتری و تجهیزات شبکه مانند سرور ، کامپیوتر ، روتر ، سویچ و ... می باشد) . (Capacity Management) -رویه های برطرف سازی و راه اندازی مجدد در صورت بروز خطا برای سیستم جدید -تست و بررسی عملکرد سیستم جدید با در نظر گرفتن استانداردهای لازم . -در نظر گرفتن کنترل های امنیتی موجود به صورتی که هیچکدام از این کنترل ها توسط سیستم جدید نقض نشوند . -وجود دستورالعمل مستند جهت استفاده موثر از سیستم جدید برای کاربران . -در نظر گرفتن تغییراتی که سیستم جدید بروی رویه های متداوم کسب و کار ایجاد می کند . -برنامه ریزی مناسب برای زمان عملیاتی شدن سیستم جدید به صورتی که در کسب و کار سازمان اختلالی ایجاد نکند . (مانند تغییر نرم افزار مالی در آخر ماه) -شناسایی ریسک هایی که با پیاده سازی سیستم جدید بوجود می آید و پیشبینی کنترل های امنیتی آن ها . -انجام آموزش های لازم جهت کاربری از سیستم جدید . در برخی موارد کسب گواهی نامه و یا تخصص لازم ، ضروری می باشد . -سهولت در کاربری از سیستم جدید که باعث بالا رفتن بازدهی و کاهش خطای انسانی می شود					

۵۱	جهت بهبود و ارتقای کیفی سیستم ها و نرم افزارهای میبایستی محیطی جهت تست و پایش در نظر گرفته شود و تحت کنترل باشد و کلیه نرم افزارها ، سیستم ها و تغییرات قبل از عملیاتی شدن در این محیط صورت گیرد و نیز نتایج آن میبایستی مستند گردد ، توصیه میشود این فرآیند شامل ارزیابی ریسک ، تحلیل پیامدهای تغییرات ، مشخصات کنترل های امنیتی مورد نیاز باشد و این فرآیند تضمین نماید که رویه های فعلی امنیت و کنترل مختل نمیشودن و برنامه نویسان دسترسی را فقط به بخشهایی از سیستم دارند که برای کار لازم است و اینکه قرارداد و تایید رسمی برای هر تغییر کسب شود .					
۵۲	الزامی میباشد تا یک رویه مدون جهت تغییر عملیاتی و عملکرد یکپارچه سیستم ها و نرم افزارها در نظر گرفته شود			سازمان		
۵۳	نرم افزارها و سیستمهای عامل باید پس از انجام تست های لازم نصب و راه انداز گردند و میبایستی تضمین این که برنامه و بودجه پشتیبانی سالانه بررسی ها و آزمون سیستم را که از تغییرات سیستم عامل ناشی می شوند پوشش خواهد داد.					
۵۴	تست ها میبایست شامل کاربرد نرم افزار ، امنیت نرم افزار ، تاثیر بر دیگر نرم افزارها و سیستم های عامل باشند . این تست ها باید بروی یک سیستم مجزا از محیط شبکه داخلی سازمان/شرکت و همانند شده با محیط واقعی کاربران انجام شود .					
۵۵	سیستم عامل تمامی سرویس دهنده ها میبایست بروز باشند و کلیه وصله های امنیتی میبایستی اعمال شوند و در این راستا میبایستی کلیه شرایط تست و پایش در نظر گرفته شوند.					
۵۶	سوابق مربوط به اینگونه تست ها میبایست ثبت و نگهداری گردند .					
۵۷	مستند سازی لازم باید برای نحوه نصب نرم افزارهای سازمانی ، سیستم عامل ها وبرنامه های کاربردی انجام شود .					
۵۸	انجام مستند سازی های لازم جهت استفاده از نرم افزارهای سازمانی با درجه اهمیت بالا .					

۵۹	نگارش های قدیمی نرم افزارهای سازمانی (Old Versions) و نرم افزارهای کاربردی با درجه اهمیت بالا باید توسط مدیر سرویس نگهداری شود.					
۶۰	Source نرم افزارهای سازمانی میبایست در مکان مناسب نگهداری شوند و این مکان (فیزیکی و یا منطقی) باید دارای حق دسترسی مناسب برای افراد مجاز باشد .					
۶۱	نصب و بروز رسانی نرم افزارها ، سرویسها و سیستم عامل ها میبایست توسط مدیران سرویس ها و یا افراد آموزش دیده زیر نظر مدیران سرویس ها انجام شود .					
۶۲	نرم افزارهای تهیه شده توسط شرکت های خارجی برای سازمان میبایست تحت نظارت و سرپرستی سازمان باشد .					
۶۳	شناسایی نقاط امنیتی و امن کردن (Hardening) سیستم های عامل و سرویس ها .					
۶۴	سرویس ها و نرم افزارهای مرتبط به سرویس اصلی همواره به روز باشند در این راستا میبایستی کلیه شرایط تست و پایش در نظر گرفته شوند مانند سرویس Apache.					
۶۵	میبایستی پورت های مربوط به سرویس ها و نرم افزارها شناسایی و پورت های بلا استفاده بسته شوند.					
۶۶	میبایستی سرویس های مورد نیاز به نرم افزارها شناسایی سرویس های بلا استفاده میبایست غیر فعال گردند .					
۶۷	استفاده نکردن از متد Plain Text Authentication در صفحه احراز هویت FTP سرور و دیگر سرویس ها.					
۶۸	استفاده از سرویس های Monitoring (مانند IPS & IDS) برای سرویس های با اهمیت سازمان مانند سرویس WEB Site.					
۶۹	تست سازگاری نرم افزارهای سازمانی با آنتی ویروس سازمان.					

۷۰	اجرای یک نرم افزار نباید نقض کننده سیاست های امنیتی سازمان باشد.					
۷۱	کلیه اطلاعاتی که به منظور انجام تست از محیط عملیاتی خارج شده و وارد محیط تستی شده اند باید تحت تدابیر امنیتی لازم قرار گیرند .					
۷۲	ایجاد Disaster Recovery برای نرم افزارهای با اهمیت سازمان .					