چک لیست تخصصی مرکز آپا دانشگاه کردستان

نام ارگان :			تاریخ تکمیل :		
ردیف	شاخه اصلی	زیرشاخه	میزان انجام فعالیت		
			کامل	تا حدودی	ناقص
۱	حفاظت از اطلاعات	حفظ حریم خصوصی داده‌های کاربران			
		طبقه‌بندی و نشانه‌گذاری داده‌های حساس و غیرحساس			
		استفاده از سیستم‌های حفاظتی برای داده‌های حساس و غیرحساس			
۲	امنیت نرم افزارها	ثبت رخدادهای امنیت نرم‌افزار			
		محدودسازی زمان‌های دسترسی کاربران به سیستم‌های نرم‌افزاری درون سازمانی			
		محدودسازی تعداد دفعات ورود ناموفق به نرم‌افزار			
		محدودسازی قابلیت ویرایش اسناد و فایل‌های نرم‌افزاری برای افراد غیرمجاز			
		تهیه نسخه پشتیبان از فایل‌ها و بانک اطلاعاتی تولید شده توسط خود نرم‌افزار			
		پیش‌بینی تهیه سیستم جایگزین برای نرم‌افزار در صورت بروز مشکل			
		نصب آخرین وصلههای نرم‌افزارها			
۳	امنیت فیزیکی	استفاده از کنترل‌های اضافی از قبیل کنترل شناسه کاربری و کلمه عبور، کنترل نشانه‌های سخت‌افزاری و یا کنترل عوامل بیومتریکی در مورد ورود به نواحی دارای طبقه‌بندی محرمانه			
		وجود رک‌های دیواری و ایستاده به تناسب تجهیزات موجود			
		داشتن اتاق سرور با شرایط استاندارد (سقف یا کف کاذب، سیستم خنک‌کننده، سیستم اطفاء حریق و مانیتورینگ)			
		قرار گرفتن سرور در اتاقی امن و کنترل تردد به این اتاق			
		وجود سیستم اعلام رویدادهای حساس			
		امن‌سازی هریک از اتاق‌ها، دفاتر، امکانات و تجهیزات جانبی مربوط به ساختمان‌ها با توجه به نواحی امنیتی تعریف شده و مطابق با الزامات آن			
		کنترل و نظارت مکان‌های حساس بطور دائم توسط دوربین‌های مداربسته و سیستم مانیتورینگ			
		استفاده از گاوصندوق‌های مخصوص جهت نگهداری و محافظت از رسانه‌های ذخیره‌سازی و نگهداری اطلاعات اعم از اطلاعات چاپی مانند فرم‌ها، نامه‌ها، مستندات مختلف و تمام مواردی که به ثبت می‌رسد.			
		استفاده از پوشش حفاظتی مناسب برای تجهیزات مخابراتی			
		استفاده از دستگاه برش و خردکن کاغذ			
		شماره‌گذاری و پلمپ تمام رایانه‌ها و تجهیزات شبکه			
		تعیین سیاست‌گذاری مناسب جهت استفاده از حافظه‌های جانبی (HDD EXT,DVD,USB)			

چک لیست تخصصی مرکز آپا دانشگاه کردستان

نام ارگان :			تاریخ تکمیل :		
ردیف	شاخه اصلی	زیرشاخه	میزان انجام فعالیت		
			کامل	تا حدودی	ناقص
۴	امنیت شبکه	افراز بخش‌های مختلف شبکه از یکدیگر بر اساس ماموریت سازمانی بخش‌ها و کارکرد اجزای شبکه			
		محدودسازی دسترسی آزاد از یک ایستگاه کاری به ایستگاه کاری دیگر، اعطای حقوق دسترسی بر اساس نیازهای کاری و تهیه فهرست‌های کنترل دسترسی			
		جداسازی فیزیکی ایستگاه‌های کاری یا شبکه‌هایی که اتصال آنها به شبکه اصلی سازمان الزام ندارد و یا به دلایل حفاظتی باید جدا نگه داشته شود.			
		محافظت از کلیه دارایی‌های اطلاعاتی مورد استفاده در فرآیند احراز هویت در مقابل دسترسی‌های غیر مجاز			
		بررسی فعالیت کاربران در جهت مقابله با تخلفاتی نظیر نصب هرگونه نرم افزار پویش پورت، پویش شبکه، عبور از فیلترینگ			
		جلوگیری از استراق سمع کاربران در شبکه			
		کنترل و بررسی سرویس‌های قابل ارائه توسط هر رایانه، غیرفعال‌سازی سرویس‌های غیر ضروری نظیر اشتراک فایل و چاپگر			
		مستند سازی نقشه شبکه، شامل نحوه اتصال فیزیکی و مسیرهای عبوری در نقاط اتصال شبکه			
		مانیتورینگ و Log برداری ترافیک عبوری از نقاط ارتباطی شبکه به‌صورت دوره‌ای در بخش های مختلف			
		استفاده از access list، محدود کننده‌های ترافیک، مکانیزم‌های اولویت‌بندی و دسته‌بندی ترافیک بر اساس مشخصات مبداء و مقصد			
		استفاده از پروتکل‌های رمزنگاری برای انتقال داده در شبکه			
		استفاده از port security بر روی سوئیچ‌های شبکه			
		استفاده از فایروال، IDS و IPS یا UTM برای تشخیص و جلوگیری از نفوذ در نقاط اتصال با شبکه‌های دیگر و یا در ایستگاه‌های کاری حساس			
		استفاده از مکانیزم تبدیل آدرس‌های شبکه(NAT) در نقاط اتصال شبکه‌های داخلی و خارجی سازمان و یا برای جداسازی و حفاظت از بخش‌های خاص شبکه			
		جداسازی بستر فیزیکی شبکه‌هایی که اطلاعات جاری در آن‌ها دارای طبقه‌بندی حفاظتی بالاتر از خیلی محرمانه است (جداسازی شبکه اداری از شبکه اینترنت)			
		جلوگیری از ایجاد و استفاده VPN، پراکسی، تونل و سایر ارتباطات غیرمجاز توسط کاربران			
۵	آموزش	آموزش و معرفی مهندسی اجتماعی			
		اطمینان از اینکه کلیه کاربران از مقررات امنیتی مربوط به اینترنت مطلع هستند.			
		آموزش به کاربران جهت استفاده صحیح از ایمیل، خودداری از دادن آدرس ایمیل به سایت‌ها و مراکز ناشناس و آموزش مقابله با هرزنامه‌های دریافتی			
		آموزش در مورد phishing			
		آموزش در سطح مبتدی درمورد پیشگیری از ورود بدافزار به سیستم‌عامل			
		آموزش‌های امنیتی ویژه و تجهیزات مناسب برای مجموعه حراست			

چک لیست تخصصی مرکز آپا دانشگاه کردستان

نام ارگان :			تاریخ تکمیل :		
ردیف	شاخه اصلی	زیرشاخه	میزان انجام فعالیت		
			کامل	تا حدودی	ناقص
۶	وب	اسکن سایت توسط یک اسکنر امنیتی خاص			
		تعیین سطح دسترسی کاربران به وب‌سایت			
		استفاده از SSL معتبر			
		استفاده از مرورگرهای امن و پیکربندی صحیح مرورگرها			
۷	ایمیل	کنترل دسترسی بیرونی به گروه‌های داخلی کاربران			
		کنترل محتوایی نامه‌ها جهت جلوگیری از خروج اطلاعات محرمانه			
		استفاده از برنامه ضد هرزنامه			
		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			
۸	بی‌سیم	آزمایش دوره‌ای نفوذ از بیرون به شبکه‌های بی‌سیم			
		استفاده از قویترین رمزنگاری ممکن			
		استفاده از شبکه رمزنگاری شده			
		بررسی وجود سیستم وایرلس بدون رمز عبور در شبکه سازمانی			
۹	سیستم‌عامل	فعال بودن UAC			
		وجود آسیب‌پذیری SMB			
		باز بودن پورت‌های مختلف			
		بررسی وجود حساب کاربری با سطح دسترسی Administrator دارای رمز عبور			
		بررسی وجود پوشه‌های Share			
		استفاده از رمز عبور پیچیده برای ورود به سیستم‌عامل			
		استفاده از فایروال و آنتی‌ویروس در سیستم‌عامل			
		به‌روزرسانی برنامه ضد بدافزار در سیستم‌عامل			
		الزام استفاده از کلمات عبور پیچیده در سیستم عامل			
		به روز بودن سیستم‌عامل و نصب بودن آخرین وصله‌های امنیتی			
		اعطای سطح دسترسی پایین برای کاربران			
		تنظیم اشتراک‌گذاری در سیستم‌عامل			
		عدم دسترسی کاربران به تنظیمات آنتی‌ویروس			
		غیرفعال کردن location			
		استفاده از سیستم فایل NTFS			
		غیرفعال بودن حالت ورود اتوماتیک			
		غیرفعال بودن RDP سرور برای کاربران			
۱۰	سیستم‌عامل سرور	پیکربندی امن و به‌روزرسانی وب‌سرویس‌ها			
		پیکربندی امن و به‌روزرسانی پایگاه داده			
		پیکربندی امن و به‌روزرسانی پلتفرم برنامه‌نویسی (مانند PHP ، ASP و ...)			
		استفاده از WAF			