

عنوان پست سازمانی: کارشناس حفاظت رایانه و فناوری اطلاعات عنوان پست سرپرست مستقیم: کارشناس مسئول حفاظت رایانه و فناوری اطلاعات جایگاه پست: ستاد ■ نام واحد ستادی: حوزه ریاست دانشگاه واحدهای محیطی □ نام واحد محیطی: نام واحد / بخش سازمانی: مدیریت حراست
--

شرح وظایف اجرایی / عملیاتی متصدی پست سازمانی	
۱	پیگیری استقرار سیستم یکپارچه مدیریت کاربران
۲	پیگیری اعمال کنترل‌های تخصصی لازم برای حصول اطمینان از صحت انتساب نقش متناسب با هویت و وظایف مبتنی بر قلمرو و مجوزهای صادره
۳	پیگیری ایجاد فرایند اصالت‌سنجی کاربران در سامانه‌ها
۴	مشارکت در تهیه مقررات و دستورالعمل‌های حفاظتی و امنیتی در تولید، نگهداری، گردش و دسترسی به اطلاعات در سیستم‌های اطلاعاتی
۵	پیگیری تدوین، نظارت و ارزیابی کنترل‌های امنیتی بر روی داده‌ها و اطلاعات به هنگام تبادل از مرزهای کسب و کار دستگاه
۶	پیگیری ایجاد پایگاه داده امن منطبق بر استانداردها و چارچوب‌های پذیرفته شده و تهیه نسخ پشتیبان از بانک‌های اطلاعاتی به صورت منظم و دوره‌ای و نگهداری آن در فضای امن متناسب با استانداردها
۷	پیگیری و مشارکت در تدوین و استقرار معماری امن بر اساس طبقه‌بندی اطلاعات دیجیتال به منظور مقابله با مخاطرات مترتب؛ نظیر نشت اطلاعات، تخریب اطلاعات و دسترسی‌های غیر مجاز
۸	جمع‌آوری شواهد و ادله جهت ارائه به مراجع ذیصلاح به شکل استانداردپذیر به منظور مقابله با جرایم سایبری، رایانه‌ای و کشف تقلب
۹	پیگیری تدوین و نظارت بر مستندسازی فرایندها و دارایی‌های اطلاعاتی و به روزرسانی دوره‌ای آنها منطبق بر استانداردهای مربوطه از جمله نظارت بر تهیه شناسنامه الکترونیکی از شبکه، سخت‌افزار و نرم‌افزار بر پایه استقرار سامانه‌های پویا و برخظ پویش شبکه
۱۰	درج و اجرای الزامات امنیتی حوزه فناوری اطلاعات شامل اخذ گواهینامه‌های امنیتی نرم‌افزارها، سرویس‌ها و سامانه‌های حراست از مراجع ذیصلاح قبل از انعقاد قرارداد
۱۱	پیگیری طراحی، توسعه و استقرار امن و یکپارچه نرم‌افزارها، سرویس‌ها و سامانه‌ها و مدیریت چرخه حیات منطبق بر استانداردها و چارچوب‌های پذیرفته شده
۱۲	پیگیری انجام آزمون‌های امنیتی حوزه فناوری اطلاعات حراست در جهت شناسایی آسیب‌پذیری‌های نرم‌افزار، زیر ساخت و سامانه‌های مرتبط با آن
۱۳	پیگیری حسن اجرای کنترل‌های حفاظتی مرتبط با سازوکارهای تبادل اطلاعات سیستمی بین حراست و شرکت‌های طرف قرارداد
۱۴	مشارکت در تدوین سیاست‌ها و اعمال محدودیت‌های مورد نیاز در نصب و اجرای نرم‌افزارها، سرویس‌ها و کارکردهای غیرسازمانی شامل پیام رسان‌ها یا شبکه‌های اجتماعی در حراست
۱۵	پیگیری اخذ تاییدیه صلاحیت پیمانکاران و مشاورین حوزه فناوری اطلاعات از مراجع ذی صلاح

۱۶	مشارکت در تدوین و اجرای راهبرد مدیریت آسیب‌پذیری، تهدید و رویداد در حوزه فناوری اطلاعات حراست
۱۷	پایش، کنترل و کاهش آسیب‌پذیری‌ها و تهدیدات بر اساس چارچوب‌ها و استانداردهای مرتبط
۱۸	ایجاد فرآیند مستمر ارزیابی مخاطرات حوزه فناوری اطلاعات حراست
۱۹	پیگیری راه‌اندازی و استاندارد سازی اتاق سرور حراست و تعیین ضوابط کلی حفاظتی آن بر اساس زیرموفه‌های مرتبط با حوزه امنیت فناوری اطلاعات
۲۰	پیگیری راه‌اندازی مراکز داده متقارن در مناطق جغرافیایی غیر هم‌اقلیم، در راستای پوشش و پشتیبانی ارائه سرویس‌های برخط و همچنین حفاظت از داده‌های حیاتی در برابر وقایع و تهدیدات طبیعی، داخلی و خارجی
۲۱	پیگیری تفکیک شبکه‌های رایانه‌ای حراست و اعمال کنترل‌های امنیتی در راستای پیشگیری از دسترسی‌های غیرمجاز به منابع شبکه شامل پورت‌های فیزیکی و منطقی سرورها، کلاینت‌ها و تجهیزات مربوطه
۲۲	مشارکت در تدوین و اجرای ضوابط حفاظتی در خصوص نقل و انتقال و امحاء سخت‌افزاری و نرم‌افزاری تجهیزات حراست
۲۳	پیگیری پیاده‌سازی استانداردهای معماری شبکه در راستای تامین امنیت و پوشش نقاط نفوذ
۲۴	مشارکت در تدوین ضوابط حفاظتی در خصوص نصب و اتصال هر نوع تجهیزات ارتباطی و الکترونیکی اعم از کارت شبکه بی‌سیم، مودم، تلفن همراه، روتر در کلیه مبادی مرتبط با شبکه دستگاه
۲۵	ارزیابی و نظارت بر سطوح مختلف سیستمی و فرآیندی سازمان (اعم از حراست و فناوری اطلاعات)
۲۶	انجام سایر امور محوله به دستور مافوق طبق قوانین و مقررات
برنامه‌ریزی / سازماندهی / نظارت / هماهنگی	
۱	نظارت بر حسن اجرای دستورالعمل‌ها، بخشنامه‌ها و آئین‌نامه‌های ابلاغی از وزارت متبوع و سایر مراجع ذیصلاح
۲	هماهنگی درون‌بخشی و برون‌بخشی با سایر واحدها و سازمان‌های مرتبط
۳	نظارت بر عملکرد کارشناسان حفاظت فناوری اطلاعات و کارشناسان حفاظت الکترونیک
۴	نظارت بر حسن اجرای مصوبات کمیته‌های مرتبط با شرح وظایف شش‌گانه حوزه حفاظت فناوری اطلاعات
۵	نظارت بر چرخه حیات هویت در سامانه‌ها از تخصیص تا حذف و ایجاد فرایندهای متناسب با آن
آموزش / پژوهش / نوآوری / بهبود کیفیت	
۱	حضور در دوره‌های آموزشی درون و برون‌سازمانی و پیگیری اجرای آن از واحدهای مرتبط ذیصلاح