باسمه تعالی

کاربرگ شماره ۱

کاربرگ آگاهسازی و توجیه حفاظتی عمومی

اینجانب .... با کدملی .... و عضویت .... شاغل در مجتمع/معاونت .... در جلسه توجیهی و آگاهسازی مورخ / / شرکت و پیرامون محورهای زیر آگاهی لازم را کسب نموده و متعهد می‌گردم ضوابط و ملاحظات حفاظتی مصرحه را رعایت نمایم.

محورهای توجیهی:

اهم الزامات حفاظتی عمومی	اهم الزامات حفاظتی مربوط به حوزه فاوا و فضای مجازی
۱. توجه جدی به رعایت حفاظت گفتار و اصل حیطه بندی؛ ۲. عدم بیان اطلاعات و ماموریت‌های کاری دانشگاه در بین اعضای خانواده، خویشاوندان و افراد غیرمرتبط؛ ۳. غیرمجاز بودن بیان اطلاعات طبقه بندی شده از طریق تلفن؛ ۴. ممنوعیت همراهی موبایل در جلسات کاری دارای طبقه بندی؛ ۵. غیرقانونی بودن اشتغال و بکارگیری افراد با دسترسی عادی در امور و مشاغل دارای طبقه بندی؛ ۶. تحویل گذرنامه به معاونت منابع انسانی دانشگاه؛ ۷. الزام به اخذ مجوزهای لازم در هنگام اقدام برای خروج از کشور با هر نوع عضویت و دسترسی؛ ۸. لزوم اطلاع‌رسانی خروج از کشور بستگان درجه یک به حفا قبل از انجام سفر؛ ۹. ممنوعیت برقراری ارتباط با اتباع بیگانه بدون اخذ مجوز تحت هر عنوان و بیان مشخصات و رزومهٔ فردی؛ ۱۰. عدم تولید اضافی اسناد سازمانی به صورت کاغذی؛ ۱۱. جلوگیری از دسترسی افراد غیرمجاز به اسناد و اطلاعات دارای طبقه بندی(حیطه بندی)؛ ۱۲. لزوم نگهداری صحیح اسناد و مدارک دارای طبقه بندی در فایل فلزی رمزدار؛ ۱۳. الزام به امحاء اسناد زائد احتمالی (دارای طبقه بندی) بر اساس مفاد آیین نامه اسناد و مدارک؛ ۱۴. عدم تردد به اماکن دارای طبقه بندی دانشگاه پیش از اخذ مجوزهای لازم؛ ۱۵. ممنوعیت فیلمبرداری و عکسبرداری از اماکن دانشگاه بدون اخذ مجوزهای لازم؛ ۱۶. عدم بیان و انتشار موضوعات مرتبط با ماموریت دانشگاه در شبکه‌های اجتماعی غیربومی؛ ۱۷. ممنوعیت ورود به دسته بندی ها و جناح های سیاسی و تبلغات له و علیه افراد در کنار حفظ بصیرت و دانش سیاسی؛ ۱۸. اهتمام به انجام بررسی های فنی و امنیتی از سوی مبادی ذیربط در خصوص اقلام و تجهیزات خریداری شده از خارج از کشور؛ ۱۹. لزوم رعایت دقیق قانون منع مداخله کارکنان در معاملات دولتی و پرهیز از ورود به موضوعات اقتصادی منع شدهٔ قانونی؛ ۲۰. اطلاع رسانی به موقع وقوع هرگونه موارد مشکوک به حفا.	۱. ممنوعیت استفاده از تلفن همراه هوشمند و ذخیره سازهای شخصی برای مستندسازی، نگهداری و جابجایی، چاپ دیتا و اطلاعات دارای طبقه بندی؛ ۲. غیرمجاز بودن اتصال شبکه های سازمانی به شبکه‌های غیرسازمانی بدون کسب مجوز و اطمینان از سلامت امنیتی؛ ۳. عدم تولید، نگهداری و تبادل اطلاعات دارای طبقه بندی و سازمانی از طریق رایانه های متصل به اینترنت و شبکه های مرتبط با آن؛ ۴. ممنوعیت اتصال هرگونه سخت افزار حاوی اطلاعات سازمانی به شبکه غیرسازمانی و اینترنت؛ ۵. عدم اتصال تلفن همراه، لپ تاپ، رایانه های شخصی و اقلام فاوایی غیرمجاز به شبکه های سازمانی؛ ۶. اطلاع رسانی هرگونه سرقت یا مفقودی رایانه همراه و هرگونه رسانه ذخیره‌ساز الکترونیکی سازمانی (فلش، لپ تاپ، انواع لوح فشرده، رایانه) حاوی اطلاعات دارای طبقه بندی و رمزکننده های بومی ن.م؛ ۷. غیرمجاز بودن فروش رایانه ها و ابزارهای ذخیره ساز استفاده شده در ن.م به هر دلیل که امکان بازیابی اطلاعات آنها وجود دارد؛ ۸. عدم ایجاد و راه اندازی شبکه اینترنت، کانال و گروه‌های اجتماعی مجازی بدون رعایت ضوابط و مقررات مربوطه در ن.م؛ ۹. ممنوعیت فک پلمپ، دستکاری، جابجایی، تعمیر و بکارگیری تجهیزات فاوایی بدون در نظر گرفتن الزامات امنیتی؛ ۱۰. غیرمجاز بودن تهیه، نصب و بکارگیری نرم افزارها بدون اخذ ارزیابی امنیتی از کمیته امنیت فاوای دانشگاه و رعایت الگوی کنترل امنیت پذیری؛ ۱۱. عدم بهره‌برداری از سخت افزارها با قابلیت بی‌سیم و باسیم بدون اخذ مجوز؛ ۱۲. ممنوعیت استفاده از صندوق پست الکترونیک شخصی جهت ارتباط و مبادله پیام با بیگانگان بدون اخذ مجوز از فرماندهی (ریاست، معاونین دانشگاه و روسای مجتمع ها) و تاییدیه ساحفا؛ ۱۳. الزام به جداسای صندوق پست الکترونیک شخصی و سازمانی جهت برقراری ارتباط با بیگانگان پس از اخذ مجوزهای قانونی لازم؛ ۱۴. لزوم رعایت دستورالعمل های ابلاغی در زمان عضویت در شبکه‌های اجتماعی و استفاده از آن برای کارکنان ن.م؛ ۱۵. ممنوعیت تجاری نمودن هرگونه پروژه، محصول و نتایج تحقیقات انجام شده با موضوعات مرتبط با ن.م و فروش آنها به خارج از ن.م بدون ملاحظات امنیتی و اخذ مجوز از مراجع ذی‌صلاح.

نام و نام خانوادگی:

امضاء و تاریخ: / /