سیاست نامه امنیتی کاربران متصل به شبکه دانشگاه رازی

حوزه فناوری اطلاعات و ارتباطات

نسخه یک - ۱۴۰۲

در راستای حفظ امنیت اطلاعات همکاران دانشگاه، حوزه فناوری اطلاعات اقدام به تدوین سیاست نامه امنیتی خود در این خصوص نموده است. اجرای مفاد عنوان شده در این سند به منظور حفظ یکپارچگی و حراست از داده‌ها و اطلاعات سیستمی همکاران گرامی امری الزامی می‌باشد.

۱. همکاران محترم می‌بایست کلمه عبور سیستم و سامانه‌های ضروری خود مانند اتوماسیون اداری، ایمیل سازمانی و غیره را با شرایط زیر انتخاب کنند:
   a. طول کلمه‌های عبور باید حداقل ۸ کاراکتر باشد.
   b. در کلمه‌های عبور از حروف و ارقام و کاراکترهای خاص (@-#-% و ...) استفاده گردد.
   c. کلمه‌های عبور، بهتر است که در دوره‌های زمانی کوتاه یک‌ماهه تغییر داده شوند.
۲. مسئولیت حفظ و حراست از نام‌کاربری و کلمه عبور سامانه‌های اداری دانشگاه و خارج از آن و نیز پاسخگویی در صورت سوء استفاده از آنها به عهده کاربر و واحد بهره بردار می‌باشد. لذا از یادداشت، ذخیره و وارد کردن آن در مقابل دید دیگران خودداری شود.
۳. همکاران می‌بایست صفحه سیستم خود را به محض ترک کردن محل کار قفل کنند.
۴. بر روی کلیه سیستم‌ها می‌بایست آنتی‌ویروس معتبر دانشگاه نصب باشد. در صورت نیاز به نصب آنتی ویروس می‌بایست به کارشناس شبکه واحد مربوطه اطلاع داده شود.
۵. همکاران از اتصال حافظه‌های جانبی مانند فلش‌دیسک های USB، هاردهای اکسترنال و یا تلفن‌های همراه به سیستم‌های اداری خودداری نمایند.
۶. کلیه اطلاعات سیستمی و توکن‌های احراز هویت به هیچ عنوان نباید عمداً یا سهواً برای اشخاص غیرمجاز افشا گردد.
۷. همکاران گرامی از نصب نرم‌افزارهای غیر ضروری و متفرقه بر روی سیستم‌های اداری اجتناب کنند.
۸. لازم به یادآوری است که استفاده از سرویس و سامانه‌های داخلی در دانشگاه نیازمند ورود و دسترسی به اینترنت نمی‌باشد، لذا به منظور استفاده از سرویس‌های داخلی، دسترسی اینترنت سیستم را قطع نمایید.

۹. از وارد کردن پست الکترونیکی دانشگاه متعلق به خود برای ثبت نام و رجیستری در سایت‌های متفرقه خودداری نمایید.

۱۰. بدون هماهنگی با حوزه فناوری اطلاعات دانشگاه هیچگونه تجهیزات شبکه ای مانند هاب، اکسس پوینت و .... به شبکه اضافه و یا جابجا نگردد.

۱۱. نصب و راه اندازی هرگونه امکانات، سرویس‌های نرم افزاری و مجازی و ... برای ارائه خدمات به خارج از دانشگاه، صرفا در محل دیتاسنتر اصلی و با مجوز حوزه فناوری اطلاعات دانشگاه می‌باشد.

۱۲. از بازکردن ایمیل های ناشناس که دارای لینک و یا پیوست می‌باشد، خودداری فرمایید.

۱۳. هر شخصی که به شبکه دانشگاه متصل شود، به صورت ضمنی مقررات و خط مشی امنیتی دانشگاه را پذیرفته است.

نکته: در صورت بروز هرگونه نقضی در روند انجام خط مشی فوق، مورد پیش آمده مورد پیگیری و بررسی قرار می‌گیرد. کلیه پرسنل و همکاران گرامی در خصوص حفظ امنیت اطلاعات و اجرای این سیاست نامه مسئول بوده و ملزم به اجرای آن می‌باشند.