شماره نسخه: ۱

تاریخ:۱۴۰۰/۳/۹

طبقه بندی:خط مشی امنیت اطلاعات

سند خط مشی حفاظت از کلمه عبور

Password Policy

اهداف کلی:

در راستای هدف کلان دفتر فاوای دانشگاه جامع علمی کاربردی مبنی بر پیروی از استانداردهای حوزه مدیریت امنیت اطلاعات، حصول اطمینان از تداوم کسب و کار و همچنین به حداقل رساندن ریسک خرابی های محتمل در اثر وقوع رخدادهای امنیتی و کاهش اثر بالقوه آنها دستورالعمل‌های مرتبط با حوزه های مختلف فناوری اطلاعات در این دفتر تدوین خواهد شد که یکی از آنها سند خط مشی حفاظت از کلمه عبور می‌باشد.

۱-مقدمه:

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از اکانت کاربران قرار می گیرند. یک کلمه عبور نامناسب ممکن است منجر به سوءاستفاده از کل شبکه شود . به همین دلیل تمام کارمندان شامل پرسنل ستاد، صف، مراکز و پیمانکاران و سایر افرادی که به سامانه‌ها دسترسی دارند مسئول انتخاب کلمه عبور مناسب و محافظت از آن هستند.

در این سند به نکاتی در مورد ایجاد کلمات عبور قوی ، محافظت از آن‌ها ، زمان انقضاء و تغییر آن‌ها اشاره می شود. در حقیقت مخاطب این سند تمام افرادی هستند که مسئول اکانت یا هر سیستمی هستند که از طریق آن به شبکه دانشگاه جامع علمی کاربردی دسترسی دارند.

۲-سیاست‌های لحاظ شده در تدوین سند خط مشی حفاظت از کلمه عبور:

- این سند توسط دفتر فاوای دانشگاه جامع علمی کاربردی تدوین شده است و در دوره های زمانی لازم یا در زمان تغییرات، مورد بازنگری قرار خواهد گرفت.
- این خط مشی امنیتی در راستای تضمین اهداف زیر است:
  - حفاظت از اطلاعات در برابر هر نوع دسترسی غیرمجاز

- تضمین محرمانگی اطلاعات
- تضمین صحت و یکپارچگی اطلاعات
- تضمین الزامات قانونی و قضایی
- تمامی موارد نقض امنیت اطلاعات واقعی و مشکوک به مدیریت دفتر فاوا گزارش شده و بشکل مبسوط مورد بازرسی فنی و در صورت نیاز از مراجع قانونی از طریق اداره کل حراست دانشگاه جامع علمی کاربردی پیگیری خواهد شد.

- همه مدیران، سرپرستان و مسئولین بخش ها در واحد ستاد و صف و همچنین مراکز موظف به اجرای این خط مشی هستند و باید از انطباق فعالیت های کارکنان زیرمجموعه خود با خط مشی ها اطمینان حاصل کنند.
- پیروی از خط مشی های امنیت اطلاعات برای همه افراد سازمان الزامی می باشد.
- منظور از اطلاعات، اطلاعات و داده‌های سازمان در تمامی فرم های آن اعم از الکترونیک و غیر الکترونیک می باشد.
- مسئولیت های امنیتی و حفاظتی دسترسی های واگذار شده در سطح admin ، به عهده شرکت پیمانکار می باشد و لازم است شرکت نسبت به محافظت از آن دقت لازم به عمل آورد.
- کاربران باید بلافاصله بعد از دریافت مجوز (نام کاربری و کلمه عبور) ، به سیستم متصل شده ، در اولین اقدام رمز عبور خود را تغییر دهند.
- چنانچه کاربری احساس کند که از مجوز ورود وی بدون اجازه استفاده می شود موظف است موارد را هر چه سریعتر به اداره فناوری اطلاعات و ارتباطات (فاوا) اطلاع دهد.
- رمز عبور محرمانه است و کاربران نباید رمز خود را در اختیار دیگران قرار دهند.
- کاربران باید راجع به استفاده شخصی از سیستم، آگاهی کامل داشته باشند.
- نقض تعهدات امنیتی یا از بین بردن ارتباطات شبکه ای به هر طریقی، ممنوع می باشد.
- مسئولیت کامل اطلاعات، اطلاعیه ها و مجوز ها صرفا متوجه صاحب آن مجوز می باشد.
- انجام هر گونه اقدامی که سبب اختلال در کارکرد سامانه گردد ممنوع می باشد.

۳-بایدها

۱. از آن چه واضح است بپرهیزید

از عباراتی مثل نام خودتان، نام کاربری، تاریخ تولد و چنین مواردی به عنوان رمز عبور استفاده نکنید.

۲. رمز عبورهای ایجاد شده به صورت اتوماتیک را تغییر دهید

اگر رمز عبور سرویس شما به صورت خودکار ایجاد شده و در اختیار شما قرار داده شده است.

۳. رمز عبور خود را یادداشت نکنید

منظور، نگه داشتن آن ها در ایمیل، اسناد روی میز، کامپیوتر یا یادداشت کردن آن هاست.

۴. در مورد سؤال و جوابهای امنیتی دقت کنید

سؤال امینتی برای این است که در صورت فراموش کردن رمز عبور، بتوانید با پاسخ دادن به آن، رمز خود را بازیابی کنید. دقت کنید که ممکن است اشخاص نزدیک به شما پاسخ برخی از این سؤال ها را بدانند.

۵. برای اکانت های مختلف، رمز عبورهای متفاوت داشته باشید

کسانی که از رمزهای عبور یکسان برای سایتهای مختلف استفاده می کنند، ساده تر از دیگران هک می شوند.

۶. رمز عبور خود را هر از گاهی تغییر دهید

کلمات عبور را حداقل هر شش ماه عوض کنید (کلمات عبور سطح سیستم که باید هر سه ماه تغییر کنند).

۷. رمز عبور قوی انتخاب کنید

رمز عبور شما باید حاوی حروف، اعداد و علائم خاص باشد. هر چه رمز عبور طولانی تر باشد، بهتر است.

۸. رمز عبور خود را فاش نکنید

هیچ کس نباید به رمز عبور شما دسترسی داشته باشد. حتی اگر یک منبع معتبر از شما درخواست رمز عبور کرد، آن را به او ندهید.

۹. امنیت خود را بروز رسانی کنید

سعی کنید آنتی ویروس سیستم شما بروز باشد و سیستم خود را هر از گاهی برای تروجان ها، نرم افزارهای جاسوسی و ... که ممکن است خود را مخفی کرده باشند چک کنید. از این قانون ساده پیروی کنید : روی چیزی که مشکوک به نظر می رسد کلیک نکنید! و از افزونه های معتبر استفاده نمایید.

۱۰. Logout کنید

سعی کنید پس از استفاده از سرویس خود، از آن خارج شوید و همچنین از اکانت خود روی کامپیوترهای عمومی استفاده نکنید.

۱۱-نکات تکمیلی:

• کلمه عبور را از طریق تلفن به هیچ کس نگویید.

• کلمه عبور را از طریق ایمیل فاش نکنید.

• به قالب کلمه عبور اشاره نکنید (مثلاً نام خانوادگی)

• کلمه عبور را هنگامی که در مرخصی هستید به همکاران نگویید.

• از ویژگی "Remember Password" یا حفظ کلمه عبور در کامپیوتر استفاده نکنید.

اگر هر اکانت یا کلمه عبور احتمال فاش و سوءاستفاده از آن می رود، به راهبر سیستم اطلاع دهید و تمام کلمات عبور را تغییر دهید.

۴-حفاظت از کلمات عبور در سطوح مختلف

• تمام کلمات عبور در سطح سیستم باید حداقل سه ماه یک بار عوض شوند.

• تمام کلمات عبور سطح کاربر (مانند ایمیل یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می شود.

• اکانت های کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانت های آن کاربر متفاوت باشد.

• کلمات عبور نباید در ایمیل ها یا سایر شکل های ارتباطات الکترونیکی درج شوند.

۵-رهنمون های انتخاب کلمه عبور مناسب

کلمات عبور ضعیف معمولاً مشخصات زیر را دارند:

• شامل کمتر از هشت حرف است.

• کلمه ای است که کاربرد عمومی دارد مانند:

نام خانوادگی، دوستان، همکاران، تاریخ های تولد و سایر اطلاعات شخصی مانند آدرس ها و شماره های تلفن.

الگوهای کلمات یا شماره ها مانند zyxwvuts، qwerty، aaabbb، ۱۲۳۳۲۱ و غیره.

کلمات عبور مناسب مشخصات زیر را دارند:

• شامل هم حروف کوچک و هم بزرگ هستند(A-Z و a-z)

• علاوه بر حروف از ارقام و نشانه ها هم در آن ها استفاده می شود مانند: ۹ و ! - ۰# $ ٪ ^ & * () _ + | ~ = ’ {} [] ; <>

@ / . ?

• حداقل هشت حرف دارند.

• بر پایه اطلاعات شخصی، اسم یا فامیل نیستند.