دولت جمهوری اسلامی افغانستان

وزارت ترانسپورت

اداره ترانسپورت جاده

ریاست تکنالوژی معلوماتی

پالیسی پسورد یا کلمه عبور

تهیه و ترتیب : ریاست تکنالوژی معلوماتی

تاریخ: 18 قوس 1398

نسخه : نهایی

خلاصه پالیسی

پسوردها یک بخش مهم امنیتی شبکه ها را تشکیل میدهند که خط مقدم حفاظت از user طلقی میشود. پسورد ضعیف منجر به تهدید و به خطر انداختن امنیت در کل شبکه وزارت میگردد. به همین ترتیب، همه کارکنان این اداره از جمله افراد خارج از بست، قراردادی ها و یا سایر افراد ذیدخل با دسترسی به سیستم شبکه این اداره مسئول گرفتن مراحل مناسب، همانطور که در ذیل آمده است، برای انتخاب و امنیت پسوردهای خود هستند.

اهداف

هدف این پالیسی، ایجاد یک استندرد برای ایجاد پسورد قوی، حفاظت از آن پسورد و مدت زمان تغییر آن میباشد.

ساحه تطبیق

محدوده این پالیسی شامل تمام کارکنان وزارت که مسئولیت حساب استفاده کننده یا هر نوع دسترسی که حمایت یا نیاز به یک پسورد دارد را در هر سیستمی که در هر وزارتخانه موجود یا به آن دسترسی داشته باشد، را در بر میگیرد.

عمومیات این پالیسی

- تمام پسوردهای System Level و user ها (به عنوان مثال پسورد ورود به کمپیوتر) باید حداقل هر 90 روز تغییر کند.
- تمامی کلمات کلیدی در پسوردهای System Level مورد استفاده باید مطابق استندرد قبول شده جهانی باشد.
- تمام پسوردهای User Level به عنوان مثال ایمیل، ویب سایت، کمپیوتر، و غیره) باید حداقل هر 90 روز تغییر کند و 10 پسورد گذشته را مجددا استفاده نکنند.
- User name با دسترسی به امتیازات Access Level باید یک رمز عبور منحصر به فرد از همه حساب های دیگر که توسط کاربر نگهداری می شود داشته باشد.
- پسورد ها نباید در پیام های ایمیل یا سایر اشکال ارتباطات الکترونیکی وارد و ارسال شوند.
- هیچ کسی حق ندارد که username و password خود را برای کسی دیگر جهت استفاده بدهد.
- تمامی پسورد های سطح کاربر، سطح سیستم و سطح دسترسی (Access Level) باید مطابق با

دستورالعمل های شرح داده شده در زیر باشند.

دستور العمل

الزامات و ضروریات ایجاد پسورد :

- ✓ **حداکثر هشت (8) کاراکتر در تمام سیستم ها باشد.**
- ✓ **یک کلمه فرهنگ لغت یا نام مناسب نباشد.**
- ✓ **با شناسه کاربر (User ID) مشابه نباشد.**
- ✓ **در حداکثر 90 روز تقویمی لغو شود.**
- ✓ **نباید با ده پیسورد (10) قبلی یکسان باشد.**
- ✓ **در حالت (Clear and Plaintext) خارج از مکان امن منتقل نشود.**
- ✓ **هنگام ورود نمایش داده نشود.**
- ✓ **اطمینان حاصل گردد که پسورد فقط برای کاربر مجاز تنظیم مجدد (Reset) می شود.**
- ✓ **پسورد باید متشکل از حروف، اعداد و سمبول باشد.**

تغییر و یا حذف پسورد

تمام حساب های کاربری دیگری که مورد نیاز نیست باید فورا حذف شوند یا غیرفعال شوند. این موضوع شامل، اما محدود به موارد زیر نیست:

- ❖ **هنگامی که یک کاربر تقاعد، ترک وظیفه، مجددا تقرر یافته، انتظار به معاش، اخراج و غیره**
- ❖ **پسورد پیش فرض باید بلافاصله بر روی تمام تجهیزات تغییر داده شود.**
- ❖ **حساب های کارمندان قراردادی، زمانی که دیگر نیازی به حساب برای انجام وظایف خود ندارند.**

هنگامی که یک پسورد دیگر مورد نیاز نیست، باید مراحل زیر را دنبال نماید:

- ❖ **کارمند باید فورا آمر مافوق یا ریس خود را مطلع کند.**
- ❖ **قراردادی باید نقطه تماس (Point of Contact) خود را اطلاع دهد.**

- آمر مافوق یا POC باید فرم حذف پسورد را پر کند و آن را به ریاست تکنالوژی ارسال نماید.
- ریاست تکنالوژی معلوماتی پسورد کاربر و یا حساب کاربر را حذف یا در حالت تعلیق قرار می دهد.
- شخص دوم از آن بخش، اطمینان حاصل نماید که پسورد حذف و حساب کاربری حذف شده یا در حالت تعلیق قرار گرفته است.
- فورم حذف پسورد در یک سیستم ایمین ثبت و ذخیره می شود.

استندرد حفاظت از پسورد

از نام استفاده کننده (User ID) خود به عنوان پسورد خود استفاده نکنید. پسورد های وزارت را با هر شخص دیگری از جمله مقامات یا افراد با صلاحیت دیگر به اشتراک نگذارید. تمام کلمات عبور باید به عنوان اطلاعات حساس و محرمانه وزارت محسوب شوند .

در اینجا یک لیست از " نباید ها " ذکر گردیده که قرار ذیل می باشد:

- پسورد را بر روی تلفن برای هر کسی نباید نشان و یا ارسال نمایید.
- یک پسورد را در یک پیام ایمیل نباید نشان و یا ارسال نمایید.
- پسورد را نباید به رئیس نشان و انتقال ندهید.
- نباید درباره یک پسورد در مقابل دیگران صحبت کنید.
- نباید به فرمت یک پسورد (به عنوان مثال "نام خانوادگی من") اشاره کنید.
- یک پسورد را نباید در پرسشنامه و فرم های امنیتی نوشته و یا نشان دهید.
- پسورد را نباید با اعضای خانواده به اشتراک گذارید.
- در حالی که در رخصتی می باشید ، پسورد را نباید به همکار خود نشان و انتقال دهید .
- از ویژگی "یادآوری پسورد" برنامه ها نباید استفاده کنید.
- پسوردها را نباید فراموش و یا آنها را در هر جای شعبه خود ذخیره کنید.
- پسورد را نباید در یک فایل بر روی هیچ گونه سیستم کمپیوتری رمزگذاری نشده (Unencrypted) ذخیره کنید.

- ❖ اگر کسی درخواست پسورد کند ، به این سند مراجعه دهید یا آنها را به ریاست تکنالوژی معلوماتی هدایت نمایید.
- ❖ اگر یک حساب کاربری یا پسورد مشکوک و یا به خطر افتاده باشد، حادثه را به ریاست تکنالوژی معلوماتی گزارش دهید و همه پسورد ها را تغییر دهید. هک یا حدس زدن پسورد ممکن است به صورت دوره ای یا تصادفی توسط هکرها و یا هر شخص دیگری انجام گیرد.
- ❖ اگر در طول یکی از این دوره ها یک پسورد حدس زده یا هک شده باشد، کاربر باید آن را تغییر دهد.

استندرد های توسعه نرم افزار

توسعه دهندگان برنامه ها باید اطمینان حاصل کنند که برنامه هایشان شامل اقدامات امنیتی زیر است:

- باید احراز هویت کاربران را بطور فردی را پشتیبانی کند نه گروهی
- پسورد را در حالت (Clear Text) و یا در هر فرمتی که به راحتی برگشت پذیر باشد (Reversible) ذخیره نگردد.
- باید نوعی مدیریت بر اساس نقش را ارائه دهد (Role Management) ، به طوری که یک کاربر بتواند عملکرد کاربر دیگری را بدون نیاز به دانستن پسورد ان انجام دهد.
- باید هر جا که امکان دارد، از سیستم کنترل دسترسی (Access Control System) ، کنترل دسترسی ترمینال(Terminal Access Controller)(+ TACACS) ، Remote Authentication Dial in User Service (RADIUS) / یا X.509 با پروتکل دسترسی سبک LDAP (LDAP)استفاده کند .

کاربران با دسترسی از راه دور (Remote Access User)

دسترسی به شبکه های وزارت از طریق دسترسی از راه دور باید با استفاده از یک شبکه خصوصی مجازی (که در آن یک پسورد و شناسه کاربر مورد نیاز است) یا یک فرم احراز هویت پیشرفته(یعنیTokens ، Biometrics، Infrastructure Key(PKI)، گواهینامه ها ، و غیره) صورت گیرد.