وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتباربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۳: کلمه عبور، مدیریت کلمه عبور و مسئولیت پاسخگویی در مقابل دسترسی

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	اسفندماه ۸۹
نگارش سند	۱
تعداد صفحات	۱۰
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R89121203

هدف:

هدف از تدوین این توصیه نامه بیان اهمیت استفاده امن، نحوه انتخاب و مدیریت کلمه عبور و مسئولیت های استفاده کننده از کلمه عبور در مورد چگونگی استفاده از آن، اعم از کلمه های عبور عادی، یک بار مصرف و یا کلمه های عبور تولید شده توسط توکن های سخت افزاری و کلمه های عبور مورد استفاده در دسترسی های ممتاز می باشد.

ضرورت:

کلمه عبور به عنوان کاراترین و در بسیاری از مواقع، تنها روش کنترل دسترسی جهت استفاده از دارایی های اطلاعاتی بکار گرفته می شود. علاوه بر آن، استفاده از این ابزار جهت دسترسی به سیستم عامل اهمیت بسیار زیادی دارد، زیرا در صورت دسترسی به سیستم عامل، دسترسی به سایر داده ها و اطلاعات آسانتر خواهد بود. حق دسترسی به سیستم عامل شبکه و ابزارهای پیکر بندی نرم افزارها یا سخت افزارها جزو حقوق دسترسی ممتاز محسوب می شود، بنابراین لازم است کلمه های عبور دسترسی به سیستم عامل شبکه یا ابزارهای پیکربندی تحت حفاظت کامل قرار گرفته و دارای استحکام کافی باشند و با استفاده از روش های امن انتخاب، مدیریت و استفاده شوند.

الزامات:

- هر کاربر بایستی دارای یک هویت واحد و منحصر به فرد باشد و بر همان اساس شناسایی گردد. این هویت می تواند بر اساس دیدگاه سیستم مدیریت امنیت هر سازمان بصورت استاندارد تدوین گردد.
- اگر کاربری درخواست دسترسی به یک بانک اطلاعاتی حاوی اطلاعات حساس را داشته باشد لازم است با استفاده از سامانه های مدیریت هویت (مانند سامانه IdM) اطلاعات هویتی وی استخراج و

قبل از اعطای حق دسترسی، صلاحیت وی را مورد بررسی قرار داد. به عنوان مثال می توان فرض کرد کاربر تقاضا کننده مدیر ارشد [مشخصه] با مجوز دسترسی محرمانه [مشخصه] باشد و دارای حق دسترسی به بانک اطلاعاتی [حقوق] جهت خواندن یا بازنویسی رکوردهای خاص در ساعات رسمی اداری [مشخصه] باشد.

- ایجاد یک کنترل کننده دامنه (Domain Controller) یا سرور کنترل دسترسی را که فقط بر اساس شناسه کاربری و کلمه عبور کار می کند نمی توان همیشه به عنوان ایجاد سیستم کنترل دسترسی پذیرفت، بلکه لازم است با توجه به الزامات عملیاتی، درجه حساسیت سازمان بهره بردار و همچنین سطح طبقه بندی اطلاعات، سیستم مدیریت دسترسی جامعی را بر اساس ترکیبی از عوامل فوق ایجاد نمود. در این حالت، هویت الکترونیک هر کاربر براساس عوامل تعیین شده در سیستم مدیریت دسترسی تعریف شده و به کار گرفته می شود.
- استفاده از سیستم مدیریت هویت بر اساس عنصر هویت دیجیتال در سازمان ها، نهادها و مراکزی با هریک از خصوصیات زیر ضروری است:

  - در صورتی که هر کاربر نیاز به کار با بیش از سه شناسه کاربری (همراه با کلمه عبور) داشته باشد.
  - اگر تخصیص و ایجاد حساب کاربری (Account) برای کاربران جدید بیش از یک روز طول بکشد.
  - اگر حذف حساب کاربری و کلید دسترسی های تخصیص داده شده به یک نفر (به هر دلیل) بیش از یک روز طول بکشد.
  - اگر دسترسی به منابع حساس و بحرانی قابل محدودسازی نباشد.
  - اگر مانیتور نمودن دسترسی یا ممیزی منابع حساس و بحرانی امکانپذیر نباشد.

- در صورتی که سازمان از طرف سازمان پدافند غیر عامل در رده حساس یا حیاتی قرار گرفته باشد.

- در هر صورت لازم است مشخصات و اطلاعات کاربر متقاضی دسترسی و دریافت کلمه عبور به طور کامل ثبت گردد.
- لازم است هنگام استخدام افراد یا عقد هر گونه قرارداد همکاری منجر به استفاده کاربر از دارایی های اطلاعاتی، الزامات کنترل دسترسی عام سازمان با تاکید بر مسئولیت های استفاده از کلمه عبور به عنوان ادله اصلی دسترسی، به اطلاع کاربر رسانده شده و سند تعهد به رعایت آنها به امضای متقاضی برسد.
- لازم است هنگام اعطای حق دسترسی به هر یک از دارایی های اطلاعاتی تحت اختیار سازمان، الزامات کنترل دسترسی خاص آن دارایی اطلاعاتی با تاکید بر مسئولیت های استفاده از کلمه عبور به عنوان ادله اصلی دسترسی، به اطلاع کاربر رسانده شده و سند مربوط به رعایت آنها به امضای وی برسد.
- لازم است حقوق دسترسی کاربر و ابزارهای دسترسی وی به دارایی اطلاعاتی مورد تقاضا به شکل امن و غیر قابل انکار بصورت مکتوب به وی اطلاع داده شود.
- لازم است کاربر بر اساس رویه های رسمی امن نسبت به دریافت و استفاده از کلمه عبور خود اقدام نماید.
- لازم است مستندات و مکاتبات مربوط به اعطای حقوق دسترسی بصورت امن نگهداری شوند.
- در صورت قطع رابطه کاری یا استخدامی کاربر به هر دلیل ممکن، لازم است این موضوع فوراً به اطلاع افراد مربوط رسیده و سریعاً نسبت به قطع حقوق دسترسی وی تصمیم گیری شود.

- هنگام ایجاد شناسه کاربری و تخصیص دسترسی نکات زیر باید مورد توجه قرار گیرد:
  - قبل از تائید دریافت کلمه عبور، باید ابزارهای دسترسی ایجاد شده و تخصیص داده شده به وی غیر فعال باشند.
  - مکانیزم قفل شدن شناسه کاربری پس از تعداد معینی تلاش ناموفق برای ورود به سیستم و یا سعی در ورود از مسیری بجز مسیر تعیین شده (در سامانه های منطبق بر مسیر های تعریف شده)، فعال و اخطارهای لازم به متصدی دارایی اطلاعاتی و مدیر امنیت ارسال گردد.
  - کلمه عبور بایستی دارای پیچیدگی کافی متناسب با سطح طبقه بندی حفاظتی دارایی اطلاعاتی مورد مراجعه باشد.
- کلمه عبور باید (حداقل) شرایط زیر را داشته باشد:
  - اولاً حداقل از شش کاراکتر تشکیل شده باشد. در سازمان ها و مراکز حساس و حیاتی (از دیدگاه پدافند غیر عامل) حداقل طول کلمه عبور باید به ترتیب هشت و ده کاراکتر باشد. ثانیا در مقابل حمله های موجود علیه کلمه عبور مقاوم باشد.
  - کاراکترها باید ترکیبی از اعداد، حروف و علائم باشند.
  - کلمه عبور به اندازه کافی پیچیده باشد و از کلمات معنا دار یا مرتبط با جایگاه کاربر مثل نام، شماره تلفن، شماره شناسنامه، سال تولد، نام اقوام و یا سایر عباراتی که به سادگی قابل حدس زدن بوده یا در فرهنگ لغات موجود است تشکیل نشده باشد.
  - بایستی در بازه های زمان از پیش تعیین شده نسبت به تغییر کلمه عبور اقدام شود. بازه زمانی تغییر کلمه عبور دسترسی های ممتاز نباید بیش از یک سوم بازه زمانی تغییر کلمه عبور دسترسی های عادی باشد.

- استفاده از کلمه عبور مشترک با سایر افراد ممنوع است.
- نوشتن کلمه عبور روی کاغذ یا قرار دادن آن زیر صفحه کلید و یا چسباندن آن به مانیتور و یا هر محل غیرقابل حفاظت دیگر ممنوع است.
- هنگام ورود کلمه عبور باید از عدم مشاهده آن توسط افراد دیگر اطمینان حاصل شود.
- استفاده از کلمه های عبور پیش فرض ممنوع است.
- استفاده بیش از یک بار از کلمه های عبور تولید شده توسط سیستم های خودکار ممنوع است.
- در صورتی که تعداد کلمه های عبور تخصیص داده شده به یک نفر بیش از سه کلمه عبور باشد ترجیحاً از روش Single Sign-on استفاده شود.

- در صورت هر گونه ظن نسبت به افشاء کلمه عبور باید فوراً کلمه عبور تغییر یابد.
- استفاده از نام کاربری یا کلمه عبور افراد دیگر ممنوع است.
- لازم است امکان تغییر سریع کلمه عبور در اختیار کاربر گذاشته شود.

- در انتخاب و استفاده از سیستم خودکار مدیریت کلمه عبور، رعایت دستورالعمل های مدون سیاستگذاری کنترل دسترسی و استفاده از کلمه عبور الزامی است. اگر قبلاً چنین دستورالعمل هایی مدون نشده باشد استفاده از سیستم خودکار مدیریت کلمه عبور مشروط به تدوین و تصویب دستورالعمل های مدون سیاستگذاری کنترل دسترسی و استفاده از کلمه عبور می باشد.
- در صورت استفاده از سیستم های خودکار جهت مدیریت استفاده از کلمه عبور لازم است:

-کاربر مجبور به استفاده از کلمه عبور باشد تا در بررسی ها و ممیزی های بعدی مسئولیت هر یک از افراد در انجام فعالیت های مختلف غیر قابل انکار باشد.

-در صورت امکان به کاربر اجازه انتخاب یا تغییر کلمه عبور اختصاصی خود را بدهد و در صورت اشتباه در ورود اطلاعات ضمن ثبت وضعیت، پاسخ مناسب را صادر نماید. (صدور پاسخ نباید منجر به شناسایی سامانه مدیریت کلمه عبور یا افشاء اطلاعات غیر ضروری شود. این گونه اطلاعات می تواند در طرح ریزی حمله به سامانه های کنترل دسترسی یا مدیریت کلمه عبور مورد استفاده قرار گیرد.)

-فقط استفاده از کلمه های عبوری را تجویز نماید که طی دستورالعمل های مربوط در خصوص آنها سیاستگذاری شده باشد.

-در صورتیکه انتخاب و تغییر کلمه عبور در اختیار کاربر گذاشته شده است، وی را مجبور به رعایت قواعد تشریح شده در مورد انتخاب کلمه عبور نماید.

-در صورتیکه کاربر خود کلمه عبور را انتخاب می نماید وی را مجبور به تغییر کلمه عبور موقت هنگام اولین دسترسی و قبل از استفاده از سیستم نماید.

-کلمه های عبور قبلی مورد استفاده کاربر را بصورت رمز شده ثبت نماید و اجازه استفاده مجدد از کلمه های عبور قبلی را به کاربر ندهد.

-هنگام ورود کلمه عبور آن را روی نمایشگر نمایش ندهد.

-فایل کلمه های عبور را در محلی جدا از داده های کاربری نگهداری کند.

-طی مراحل نصب نرم افزار، کلمه عبور پیش فرض برنامه نویس را تغییر دهد.

- کلمه عبور مربوط به دسترسی ممتاز فقط باید بر اساس نیاز و حسب مورد و یا در مواقع ضرورت که به تائید مدیر امنیت اطلاعات برسد، اعطاء شود.
- لازم است افرادی که ممکن است نیاز به کلمه عبور مربوط به دسترسی ممتاز داشته باشند از قبل شناسایی شده و دلایل نیاز ایشان مورد تحقیق قرار گیرد. تعداد این افراد باید محدود باشد.

- روش های تولید نرم افزار و همچنین اجرای عادی نرم افزارهای کاربردی باید به نحوی باشد که هیچ کاربری نیاز به استفاده از دسترسی ممتاز نداشته باشد.
- برای حفظ یکپارچگی روش اعطای دسترسی ممتاز و به حداقل رساندن خطای انسانی از چک لیست ها و فرآیندهای از پیش طراحی شده برای پردازش فرآیند تخصیص دسترسی ممتاز و کلمه عبور مربوط به آن استفاده شود.
- حتی الامکان باید از مدل OTP (One Time Password – کلمه عبور یک بار مصرف) جهت اختصاص دسترسی ممتاز استفاده شود.
- در سیستم هایی که حقوق دسترسی ممتاز بصورت پیش فرض تخصیص داده می شود، لازم است نام کاربری پیش فرض تغییر داده شود (به عنوان مثال در سیستم عامل ویندوز نام کاربری پیش فرض Administrator به نامی دیگر تغییر داده شود).
- بطور کلی استفاده از نام های کاربری پیش فرض ممنوع است.
- در سیستم هایی که نیاز به حق دسترسی ممتاز دارند بایستی حداقل دو کاربر با دسترسی ممتاز ایجاد شود که یکی از آنها در مواقع اضطراری به عنوان پشتیبان به کار گرفته شود.
- لازم است حقوق دسترسی ممتاز بصورت دوره ایی (حداقل هر ۶ ماه یکبار) مورد بازنگری قرار گرفته و بهره برداری از شناسه های کاربری و کلمه عبور کاربران دارای حق دسترسی ممتاز بصورت مضاعف مورد کنترل قرار گیرد.
- لازم است استفاده از کلیه شناسه های کاربری از طریق اعمال مقررات محدودیت زمان نشست و محدودیت زمان اتصال تحت کنترل قرار داشته باشد.

- در صورت نیاز به انتقال کلمه عبور در شبکه لازم است از ارسال آن به صورت رمزنشده خودداری شده و از الگوریتم های مناسب و مستحکم رمزنگاری برای حفاظت استفاده شود.

- در صورت نیاز به نگهداری و ذخیره سازی کلمه عبور (به هر دلیل ممکن) نیز رمزگذاری آن ضروری است.

- تا زمانی که کاربر اعلام نکرده است که شناسه کاربری، کلمه عبور و یا ابزارهای اثبات هویت سخت افزاری را بصورت امن دریافت کرده، تمام دسترسی ها و شناسه های کاربری باید غیر فعال باقی بمانند تا سوء استفاده احتمالی از آنها امکان ناپذیر باشد.

- هر یک از کاربران و یا مراجعه کنندگان به دارایی های اطلاعاتی که موظف به استفاده از کلمه عبور جهت دسترسی به دارایی اطلاعاتی مورد درخواست می باشند در خصوص رعایت این دستورالعمل دارای مسئولیت می باشند.

- مسئولیت اطلاع رسانی در خصوص نحوه استفاده امن از کلمه های عبور به عهده مدیر امنیت اطلاعات و یا نهاد جایگزین آن می باشد.

- مسئولیت تدوین روش ها و مقررات استفاده امن از کلمه عبور به عهده مدیر امنیت اطلاعات و یا نهاد جایگزین آن می باشد.

- مسئولیت تعیین ضوابط انتخاب و نوع استفاده از کلمه های عبور و نظارت بر اجرای آنها به عهده مدیر امنیت اطلاعات یا نهاد جایگزین آن می باشد.

- مسئولیت تعیین شرایط و ضوابط تخصیص دسترسی های ممتاز به دارایی های اطلاعاتی به عهده مدیر امنیت اطلاعات یا نهاد جایگزین آن می باشد.

- مسئولیت درخواست ایجاد حساب کاربری به عهده مسئول مستقیم کاربری است که تقاضای دسترسی به دارایی های اطلاعاتی را دارد.

- مسئولیت تائید یا رد درخواست دسترسی به عهده متصدی دارایی اطلاعاتی مورد درخواست می باشد.

- مسئولیت بررسی و انطباق شرایط کاربر با معیارهای امنیت اطلاعات سازمان و تصویب یا عدم تصویب آن به عهده مدیر امنیت اطلاعات یا نهاد جایگزین آن می باشد.

- مسئولیت انتخاب مکانیزم دسترسی به هر دارایی اطلاعاتی از بین مکانیزم های تصویب شده به عهده متصدی یا تحویل گیرنده یا مالک همان دارایی اطلاعاتی می باشد.

- مسئولیت انتخاب، تخصیص، نگهداری و تغییر کلمه های عبور و همچنین استفاده از آن بر عهده کاربر متقاضی استفاده از کلمه عبور می باشد.

فرآیند:

بهترین روش برای اطمینان از آگاهی کاربر نسبت به اهمیت نحوه استفاده از کلمه عبور و یا هر گونه مکانیزم احراز هویت، امضای سند کتبی مبین الزامات استفاده از کلمه عبور پس از مطالعه آن می باشد. پس از این کار می توان شناسه کاربری و کلمه عبور یا تجهیزات مربوط به احراز هویت را به وی تحویل داد.

همچنین لازم است کاربر دریافت کلمه عبور خود را به متصدی دارایی اطلاعاتی اطلاع دهد. در روش های خودکار تخصیص کلمه عبور باید کاربر ملزم به تغییر کلمه عبور در اولین مراجعه به دارایی اطلاعاتی باشد. فعال سازی حساب کاربری و اعطای حقوق دسترسی به وی پس از اطمینان از دریافت امن کلمه عبور توسط کاربر مجاز خواهد بود. تغییر کلمه عبور در سیستم های تخصیص خودکار کلمه عبور به منزله اعلام دریافت کلمه عبور اولیه توسط کاربر تلقی می گردد.

ممکن است در برخی از موارد درک درستی از لزوم حفظ محرمانگی کلمه عبور وجود نداشته باشد و افراد بدون توجه به پیامدهای خطرناک افشای کلمه عبور نزد افراد دیگر به این کار مبادرت کنند. برای مقابله با این پدیده خطرناک، اطلاع رسانی به افراد و آگاهی بخشی در خصوص تهدیدهای مرتبط با آن و اطمینان از تاثیر

این فعالیت ها ضروری است. بعلاوه لازم است در دوره های آموزشی مختلفی که در مورد استفاده از دارایی های اطلاعاتی یا امنیت اطلاعات برگزار می شود به این موضوع پرداخته شود. همچنین لازم است در مواقع ضروری از اقدامات انضباطی و یا پیگرد قانونی برای مقابله با کوتاهی در زمینه حفظ محرمانگی کلمه عبور استفاده شود. در این صورت لازم است اولاً آموزش های رسمی مربوط در اختیار کاربر قرار گرفته باشد و ثانیاً هنگام تسلیم کلمه عبور به کاربر، التزام وی به حفظ محرمانگی آن اخذ شده و پیامد های نقض آن به اطلاع وی برسد.

تعاریف:

هویت دیجیتال: هویت هر شخص را می توان بصورت مجموعه ای از مشخصه های سازمانی وی (مثل بخشی که درآن کار می کند، وظیفه سازمانی وی، مدارک تحصیلی وی و....)، حقوق سازمانی وی (مثل منابعی که در اختیار وی است، حدود اختیارات وی در سازمان و...)، شناسه کاربری و کلمه عبوری که در اختیار دارد و همچنین خصوصیات فیزیکی وی (مثل اطلاعات بیومتریک، قد، وزن، سن، جنس و غیره) تعریف کرد.