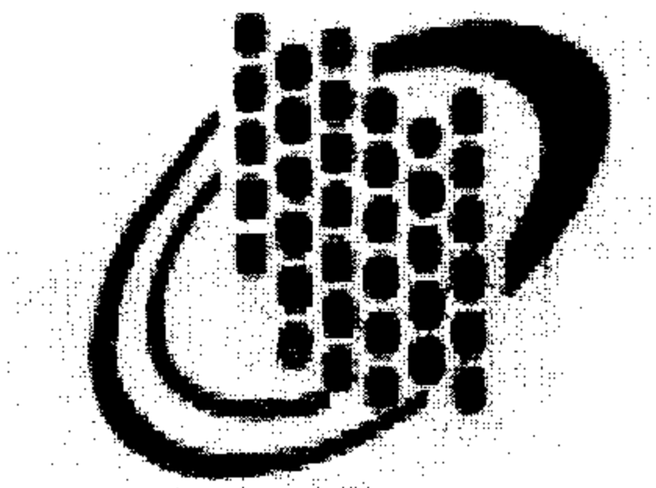

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات و ارتباطات

توصیه نامه شماره ۲:

بخش کنترل دسترسی از مجموعه

کنترل دسترسی، کلمه عبور، مدیریت کلمه عبور و

مسئولیت پاسخگویی در مقابل دسترسی

دی ماه ۱۳۸۹

هدف:

هدف از تدوین این توصیه نامه بیان لزوم سیاستگذاری کنترل دسترسی منطقی به دارایی های اطلاعاتی تحت مالکیت آن دستگاه می‌باشد.

ضرورت:

کنترل دسترسی مهمترین جزء در برقراری امنیت اطلاعات است زیرا مکانیزم های کنترل دسترسی، اولین رده دفاعی را در مقابل دسترسی غیر مجاز به دارایی های اطلاعاتی تحت حفاظت تشکیل می دهند.

مکانیزم های کنترل دسترسی قابلیت کنترل، محدودسازی، آشکارسازی و حفاظت از منابع سازمان را در جهت حفظ دسترسی پذیری، جامعیت و محرمانگی در اختیار استفاده کننده از آن می گذارد.

الزامات:

- در صورت صدور هر گونه قانون، مقررات یا دستورالعمل سازمانی مربوط به حفاظت از اطلاعات یا نحوه دسترسی پذیری به آن، لازم است بلافاصله مفاد این توصیه نامه بر اساس قانون، مقررات یا دستورالعمل جدید، بهنگام سازی شود.
- لازم است حقوق دسترسی کلیه افراد دارای حق دسترسی از قبیل کارکنان، پیمانکاران و کاربران شخص ثالث به دارایی های اطلاعاتی، به محض خاتمه استخدام یا قرارداد یا ارتباط کاری، حذف شده یا به محض تغییر شکل مورد بازنگری قرار گیرد.
- صدور اجازه دسترسی به هر متقاضی دسترسی به دارایی های اطلاعاتی، فقط پس از احراز هویت و صلاحیت متقاضی مجاز خواهد بود.
- در طراحی روش احراز هویت لازم است به عوامل زیر توجه شود:
  - طبقه بندی حفاظتی اطلاعات مورد درخواست

- امکان اعمال مدیریت متمرکز کنترل دسترسی
- طراحی فرآیند پردازش درخواست دسترسی متناسب با طبقه بندی حفاظتی اطلاعات مورد درخواست
- لازم است کنترلهای ذیل بر روی شناسه های کاربری اعمال گردد:
  - برای هر کاربر، شناسه کاربری (User ID) مجزا تخصیص داده شود.
  - استفاده اشتراکی از شناسه کاربری یا تخصیص یک شناسه کاربری به چند نفر اکیداً ممنوع می باشد.
  - به هر کاربر فقط حق دسترسی به دارایی های اطلاعاتی داده شود که برای انجام کار خود به آن نیاز دارد. دادن حق دسترسی به سایر اطلاعات یا دارایی های اطلاعاتی ممنوع است.
  - دسترسی کاربران به دارایی های اطلاعاتی فقط در ساعات کار رسمی اداری مجاز و در غیر این ساعت ها ممنوع است، مگر آنکه مجوز کتبی آن قبلاً صادر شده باشد.
  - لازم است شناسه های کاربری بدون استفاده یا متروک از سیستم حذف شود.
  - استفاده از شناسه های کاربری عمومی (مثل شناسه های کاربری مورد استفاده در اتصال به اینترنت در مکان های عمومی) فقط پس از اثبات دلیل نیاز به استفاده از آن و کسب مجوز کتبی از مقام مسئول مجاز است.
  - در صورت استفاده از شناسه های کاربری عمومی لازم است فهرست گیری (Log) از فعالیت های انجام شده به نحوی باشد که حتی الامکان در صورت نیاز بتوان به فردی که از آن شناسه استفاده کرده است دست یافت.

- در سازمان ها، نهادها یا مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس شناسایی شده اند، لازم است علاوه بر کلمه عبور، از توکن های سخت افزاری (مثل USB Token و یا Smart Card) نیز استفاده شود.
- در سازمان ها، نهادها یا مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حیاتی شناسایی شده اند لازم است علاوه بر روش های فوق از روش های کنترل دسترسی بیومتریک استفاده شود. هنگام استفاده از این روش کنترل دسترسی باید به استحکام روش احراز هویت از طریق شناسایی اثر انگشت (Finger Print)، شناسایی الگوی چهره یا چشم (Facial/Eye Pattern) یا الگوی صدا (Voice Pattern) توجه شود.
- هنگام دسترسی به ابزار مدیریت و کنترل اطلاعات دارای طبقه بندی حفاظتی خیلی محرمانه یا بالاتر، لازم است از روش احراز صلاحیت دو مرحله ای (تائید صلاحیت دسترسی از طرف مقام بالاتر و یا دسترسی به اطلاعات با حضور مسئول هم رده) استفاده شود.
- لازم است در طراحی روش کنترل دسترسی به عوامل زیر نیز توجه شود:
- اعمال کنترل های اضافی صدور مجوز دسترسی برای افراد ثالث یا اشخاصی که دارای رابطه استخدامی با سازمان نیستند
- توجه به مکان استقرار دارایی اطلاعاتی یا مکان دسترسی (دسترسی راه دور یا خارج از محیط سازمان)
- تشکیل و مدیریت فهرست کنترل دسترسی (Access Control List) یا به عبارت ساده تر ACL
- اعطای دسترسی بر اساس مسئولیت/ پاسخگویی

- لازم است کاربرها به دسته های زیر یا دسته بندی های دیگری که با حوزه فعالیت سازمان متناسب باشد، تقسیم بندی شده و در صورت وجود هر یک از دسته ها، نسبت به تدوین روش اعطای دسترسی به هر یک تصمیم گیری شود:
  - کاربران متقاضی دسترسی ممتاز (Privileged Access)
  - کاربران عادی
  - شرکای تجاری یا همکاران دولتی
  - تهیه کنندگان/ ارائه کنندگان خدمات/ پیمانکاران/ کارمندان موقت
  - بازدید کنندگان یا مراجعه کنندگان
- دسترسی به برنامه های کاربردی باید بر اساس مدل دسترسی سه سطحی کنترل دسترسی عام، کنترل دسترسی خاص و کنترل دسترسی ممتاز به شرح زیر مدیریت شود:

(انتخاب و پیشنهاد نوع مکانیزم یا مکانیزم های کنترل دسترسی در هر سطح به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات ویا نهاد جایگزین وی وتصویب آن به عهده بالاترین مقام اجرایی سازمان خواهد بود.)

- دسترسی به هر برنامه کاربردی جهت مشاهده یا بهره برداری از اطلاعات فقط پس از طی فرآیند تخصیص دسترسی عام مجاز خواهد بود.
- دسترسی به هر برنامه کاربردی جهت تغییر در اطلاعات موجود در آن نرم افزار یا بانک های اطلاعاتی مرتبط با آن فقط پس از طی فرآیند تخصیص دسترسی خاص مجاز خواهد بود.

- دسترسی به هر برنامه کاربردی، بانک اطلاعات، سیستم عامل، تجهیزات پردازشی یا مسیریابی یا ذخیره سازی و یا هر گونه دارایی اطلاعاتی دارای طبقه بندی حفاظتی خیلی محرمانه یا بالاتر ویا جهت تغییر در پیکربندی آن دارایی اطلاعاتی فقط پس از طی فرآیند تخصیص دسترسی ممتاز مجاز خواهد بود.
- دسترسی به بانک های اطلاعاتی به منظور تغییر در محتوای آن فقط پس از طی فرآیند تخصیص دسترسی خاص مجاز خواهد بود.

- لازم است در خصوص کنترل دسترسی و استفاده از هریک از تجهیزات زیر تصمیم گیری شود:
  - تجهیزات پردازش همراه، PDA یا تلفن های هوشمند
  - تجهیزات ذخیره سازی همراه (پرتابل)، درایوهای USB و یا لوازم مشابه
  - فلاپی دیسک، CD، DVD و یا تجهیزات مشابه
  - تجهیزات امانی که به صورت موقت از طرف هر مرجعی در اختیار سازمان قرار گرفته باشد (مثل مودم ها، مسیریاب ها یا سوئیچ ها، بریج ها، تجهیزات ارسال و دریافت ماهواره ایی و یا سایر تجهیزات متعلق به سرویس دهنده های مخابراتی یا پردازشی)
- علاوه بر الزامات فوق لازم است برای جلوگیری از دسترسی های ناخواسته، ممانعت از ایجاد امکان عبور غیر مجاز از مکانیزم های کنترل دسترسی، جلوگیری ازایجاد فرصت حمله به سیستم هایی که بر اثر حمله های مبتنی بر فروپاشی سیستم و دور زدن ابزار کنترل دسترسی آسیب پذیر هستندو همچنین پیشگیری از روش های بی اثر کردن سیاستهای کنترل دسترسی به موارد زیر توجه شود:
  - فقط سخت افزارهای پردازشی یا ارتباطی دارای مجوز بکار گرفته شود و نصب آنها توسط افراد معتمد انجام پذیرد.

- نصب مودم اعم از مودم کابلی یا بی سیم یا ماهواره ممنوع است مگر آنکه قبلاً مجوز آن توسط واحد امنیت اطلاعات صادر شده باشد. نصب مستقیم مودم به شبکه داخلی سازمان ممنوع است.
- دسترسی به فایل های پیکربندی نرم افزارها و سخت افزارها بایداز طریق اعمال کنترل دسترسی ممتاز، تحت کنترل کامل قرار گیرد.
- استفاده از تجهیزات USB یا حافظه های Flash برای جابجایی اطلاعات شبکه داخلی یا سایر اطلاعات دارای طبقه بندی حفاظتی ممنوع می باشد. در صورت ضرورت استفاده از این نوع تجهیزات، لازم است از مکانیزم های رمزنگاری اطلاعات استفاده شود.
- در صورت سرقت یا مفقود شدن هر یک از دارایی های اطلاعاتی لازم است روش های کنترل دسترسی که ممکن است به دلیل دستیابی افراد غیر مجاز به آن دارایی اطلاعاتی افشاء شوند، مورد بازبینی قرار گرفته و در صورت نیاز تغییر یابند.
- لازم است کلیه نرم افزارهای اضافی یا غیر ضروری موجود در شبکه داخلی سازمان، بخصوص نرم افزارهای مدیریتی (مدیریت دسترسی، مدیریت ریسک، مدیریت اطلاعات) و برنامه نویسی حذف گردند.
- دسترسی به نرم افزارهای انتقال فایل (مثل FTP، TFTP، RARP و غیره) محدود گردد.
- اجرای دستور در سطح سیستم (مثل دستورهای سیستم عامل) فقط به افراد خاصی که از طریق اعمال سیاست کنترل دسترسی ممتاز، حق دسترسی به سیستم را دارند محدود گردد.
- کنترل دسترسی به فایروال، IDS، آنتی ویروس، سیستم احراز هویت یا اعتبارسنجی، کنترل ورود به سیستم (Active Directory) و دیده بانی و مانیتورینگ سیستم باید جزو دسترسی های ممتاز محسوب شده و کنترل های لازم در مورد آن اعمال گردد.

- هر گونه نقص در عملکرد سیستم های کنترل دسترسی یا حمله به آنها به عنوان حادثه ای مهم تلقی شده و فوراً مورد رسیدگی قرار گرفته و ترمیم شود.

فرآیند:

کنترل دسترسی باید بر اساس نوع و ماهیت دارایی اطلاعاتی موضوع دسترسی، هویت متقاضی دسترسی و صلاحیت وی برای دسترسی انجام پذیرد.

طبقه بندی حفاظتی دارایی اطلاعاتی، تعیین کننده نوع و ماهیت دارایی اطلاعاتی از دیدگاه اعطای حقوق دسترسی و روش کنترل آن است. بدیهی است هر چه سطح طبقه بندی دارایی اطلاعاتی مورد نظر بالاتر باشد باید اعطای حقوق دسترسی با دقت بیشتری انجام پذیرفته و مکانیزم های کنترل آن سخت گیرانه تر باشد.

صلاحیت کاربر (اعم از انسان و یا نهاده ای که درخواست دسترسی به اطلاعات را دارد) بر اساس نوع و ماهیت دارایی اطلاعاتی تعیین می گردد. به عبارت دیگر خصوصیات و قابلیت های متقاضی جهت دسترسی به هر دسته از دارایی های اطلاعاتی باید قبلاً تعیین شود. به عنوان مثال یکی از قواعد دسترسی به فایل های پیکربندی تجهیزات مسیریابی را می توان به شرح زیر مکتوب کرد:

"دسترسی به فایل پیکربندی مسیریاب اصلی شبکه سازمان الف فقط برای مدیر شبکه سازمان الف و جانشین وی مجاز می باشد".

به عبارت دیگر هیچ یک از افراد، بجز دو فرد فوق، صلاحیت دسترسی به فایل پیکربندی مسیریاب را ندارند.

بنابر مواد فوق لازم است کلیه افرادی که تقاضای دسترسی به یک دارایی اطلاعاتی تحت حفاظت را دارند اولاً احراز هویت شده و سپس در صورت صلاحیت دسترسی به آن دارایی اطلاعاتی، امکان دسترسی به آن را پیدا نمایند.

احراز هویت افراد یا نهاده های متقاضی دسترسی بر اساس تشخیص عوامل زیر انجام می شود:

- هویتی که ادعا می شود (شناسه کاربری)
- آنچه که اثبات کننده ادعا است (کلمه عبور)
- آنچه که همراه دارد (توکن سخت افزاری)
- آنچه که هست (اثر انگشت، الگوی عنبیه یا صورت یا سایر پارامترهای بیومتریک)
- آنکس که گفته وی را تائید می کند (مقام بالاتر یا عامل قانونی)

استفاده از دو عامل اول در احراز هویت ضروری و اجباری می باشد.

جهت اعمال کنترل های بیشتر (در حفاظت از دارایی های با طبقه بندی حفاظتی بالاتر) لازم است از سایر عوامل یا ترکیبی از عوامل دیگر (بر اساس سطح طبقه بندی یا حساسیت دارایی اطلاعاتی) استفاده نمود.

تعاریف:

کنترل دسترسی عبارت است از روشی که طی آن نحوه برقراری ارتباط یا تعامل بین کاربران و سیستم ها با سایر سیستم ها یا منابع (اعم از اطلاعاتی، پردازشی، ذخیره سازی و ارتباطی) کنترل می شود. هدف اصلی در کنترل دسترسی جلوگیری از دسترسی غیر مجاز به اطلاعات بوده و همچنین می تواند در تعیین حدود حوزه اختیار متقاضی دسترسی به منبع مورد نظر (پس از طی موفق مرحله اعتبار سنجی) به کار گرفته شود.

شناسایی[1] عبارت است از اطمینان از اینکه هر نهاده (کاربر، برنامه یا فرآیند) همان موجودیتی است که ادعا می شود. ساده ترین راه اثبات ادعا و شناسایی، استفاده از شناسه کاربری و کلمه عبور می باشد.

[1] Identification

در صورت بررسی و اثبات وجود حق یا امتیاز دسترسی به منبع یا منابع مورد نظر بر اساس بررسی اطلاعات موجود نزد موضوع، اختیار دسترسی به نهاده تفویض می شود این مرحله تفویض اختیار[1] نام دارد.

کنترل دسترسی عام به معنی تعیین شرایط عامی است که باید در دسترسی افراد به هر دارایی اطلاعاتی مورد توجه قرار گیرد.

کنترل دسترسی خاص به معنی تعیین شرایط کاربرانی است که اجازه دسترسی به داده های تحت کنترل سامانه را (با توجه به حوزه اختیارات خود) دارند. به عنوان مثال ممکن است کاربر اجازه دسترسی به بخشی از داده‌های طبقه بندی شده و یا تغییر در بخش هایی از داده ها را داشته باشد. البته در کلیه موارد فوق توجه به صلاحیت کاربر و رعایت اصل پاسخگویی ضروری است.

کنترل دسترسی ممتاز به معنی تعیین شرایط دسترسی افرادی است که حق تغییر در پیکربندی نرم افزار یا سرویس های مختلف را (باتوجه به صلاحیت و پاسخگویی خود) دارند. به عنوان مثال حق تعریف کاربران در سیستم عامل ها یا تغییر در پیکر بندی بانک های اطلاعاتی به عنوان حق دسترسی ممتاز شناخته می شود.

[1] Authorization