به نام خدا

راهنمای تولیدکننده

اسفند ماه ۹۳

نسخه ۱,۰

پیشگفتار

با رشد روز افزون تهدیدات در فضای تولید و تبادل اطلاعات، مسئله امنیت جایگاه ویژه‌ای پیدا کرده است. بدین جهت تولیدکنندگان محصولات فضای تولید و تبادل اطلاعات، سعی در تولید محصولاتی دارند که با تهدیدات موجود مقابله نماید. در این راستا تولیدکننده ادعا می‌نماید که محصول دارای کارکرد امنیتی است. بنابراین باید مرجعی ادعای تولید کننده را بررسی و برای محصول گواهی صادر نماید.

در این سند که برای تولیدکنندگان محصول تهیه شده، روال ارزیابی و مسئولیت‌های تولیدکننده و تعاملاتش با آزمایشگاه، سازمان فناوری اطلاعات و مرکز افتا شرح داده شده است.

فهرست

مقدمه

هدف از این سند راهنمایی و کمک کردن به تولید کننده‌ای است که از سازمان فناوری اطلاعات درخواست ارزیابی محصول خود را کرده است تا نسبت به مسئولیتش پیش از، در طول و پس از ارزیابی شناخت کافی پیدا و آمادگی لازم را ایجاد نماید. علاوه بر این روابط تولیدکننده با آزمایشگاه، سازمان فناوری اطلاعات و مرکز افتا در این سند بیان شده است.

این سند یکی از مجموعه اسناد تهیه شده توسط مرکز افتا برای شرح چگونگی عملکرد «طرح ارزیابی امنیتی» برای تولیدکنندگان محصولات حوزه فتا می‌باشد و شامل سه فصل اصلی به شرح ذیل می‌باشد:

فصل اول: معرفی اصطلاحات و تعاریف
فصل دوم: ارائه دیدکلی از فرآیند ارزیابی استاندارد ارزیابی معیار مشترک
فصل سوم: ارائه راهنمای تولیدکننده

۱ کلیات

۱,۱ اصطلاحات

مرجع اصطلاحات بکار رفته در این سند، سند «طرح ارزیابی امنیتی» می‌باشد.

۲,۱ نقش‌ها در ارزیابی امنیتی محصولات

به منظور برقراری امنیت در محصولات فناوری اطلاعات، مرکز افتا سندی تحت عنوان «طرح ارزیابی امنیتی» تدوین نموده تا انطباق محصولات فناوری اطلاعات و پروفایل‌های حفاظتی را بر استاندارد ارزیابی معیار مشترک بررسی نماید.

شرکت‌کنندگان اصلی در «طرح ارزیابی امنیتی» عبارتند از:

- تولید کننده

تولید کننده محصول یا پروفایل حفاظتی، از سازمان فناوری اطلاعات و سپس آزمایشگاه معرفی شده توسط مرکز افتا درخواست ارزیابی محصول یا پروفایل حفاظتی می‌نماید.

- آزمایشگاه

آزمایشگاه براساس سند «اعتباربخشی آزمایشگاه» و توسط مرکز افتا اعتباربخشی و تائید می‌شود تا براساس استاندارد ارزیابی امنیتی معیار مشترک و با استفاده از متدلوژی ارزیابی معیار مشترک، ارزیابی امنیتی انجام دهد.

- مرکز افتا

مرکز افتا یک نهاد دولتی است که براساس «طرح ارزیابی امنیتی» عمل می‌نماید و ارزیابی‌های انجام شده توسط آزمایشگاه را نظارت و اعتباربخشی می‌نماید. در ارزیابی محصولات وظیفه اصلی مرکز افتا نظارت و اعتبارسنجی ارزیابی‌هایی است که توسط آزمایشگاه انجام می‌گیرد. خدمات مرکز افتا عبارتند از:

- تائید منطبق بودن ارزیابی و تست محصول با مفاد سند «طرح ارزیابی امنیتی» و استاندارد ارزیابی معیار مشترک
- حصول اطمینان از معتبر بودن نتایج ارزیابی امنیتی که توسط آزمایشگاه انجام شده
- برگزاری جلسات فنی
- تعیین آزمایشگاه برای ارزیابی محصول با مشارکت سازمان فناوری اطلاعات
- نظارت فرآیند ارزیابی محصول در آزمایشگاه
- تدوین پروفایل حفاظتی
- پاسخ به سوالات مشتریان
- بررسی و پاسخگویی به شکایات

- سازمان فناوری اطلاعات

سازمان رابط بین مرکز افتا، تولیدکنندگان و آزمایشگاه-هایی است که خواستار اعتباربخشی شدن هستند. سازمان فناوری اطلاعات منتشر کننده اطلاعات عمومی مربوط به محصول بر روی سایت سازمان می‌باشد. خدمات سازمان فناوری اطلاعات عبارتند از:

- ارائه منابع آموزشی
- اطلاع رسانی آخرین اطلاعات در رابطه با فرآیندها و روال‌های طرح ارزیابی امنیتی
- اطلاع رسانی آزمایشگاه‌های مورد تائید مرکز افتا و هرگونه تغییر در آزمایشگاه
- اطلاع رسانی محصولات تائید شده همراه گواهی و مستندات مربوطه
- اطلاع رسانی لغو گواهی
- اطلاع رسانی پروفایل‌های حفاظتی تدوین شده
- ارائه راهنما در رابطه با نوع مدارک مورد نیاز برای ارزیابی
- انتشار گواهی صادر شده محصولات همراه مستندات مرتبط
- انتشار و نگهداری لیست محصولات معتبر، ارائه جزئیات تمام محصولات و پروفایل‌های حفاظتی ارزیابی شده و گواهی‌های صادر شده
- انتشار لیست محصولات تحت ارزیابی

لازم به ذکر است مرکز و سازمان نقشی در ارائه خدمات جهت آماده نمودن تولیدکننده برای ارزیابی یا جمع‌آوری و آماده نمودن مدارک مورد نیاز ندارند.

۳,۱ ساختار سند

مجموعه اسنادی که در مرکز افتا تهیه شده و این سند تکمیل کننده آنهاست عبارتند از:

سند ۱: طرح ارزیابی امنیتی

سند ۲: سند نظامنامه کیفیت

سند ۳: راهنمای اعتبارسنج

سند ۵: راهنمای آزمایشگاه

سند ۶: تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد

سند ۷: راهنمای نوشتن پروفایل حفاظتی/سند هدف امنیتی

سند ۸: راهنمای اعتباربخشی آزمایشگاه‌ها

پیش از شروع ارزیابی، تولید کننده ممکن است سوالاتی راجع به طرح ارزیابی امنیتی داشته باشد، بدین منظور باید مستندات راهنمای مرکز افتا (اشاره شده در بالا) را مطالعه یا به بخش سوالات رایج در سایت سازمان مراجعه نماید.

۲ دیدکلی ارزیابی استاندارد معیارمشترک

یکی از نیازهای مصرف کنندگان محصولات فناوری اطلاعات وجود مرجعی قابل اطمینان است که محصولات را ارزیابی نماید، تا با استناد به نتایج ارزیابی بتوانند به قابلیت‌های امنیتی محصولات اعتماد نمایند و بدین ترتیب محصولات مختلف را با یکدیگر مقایسه و قابلیت‌ها و محدودیت‌های آنها را درک نمایند.

طرح ارزیابی امنیتی استاندارد معیار مشترک به واسطه یک نهاد مستقل، ارزیابی بی طرفی از محصول را برای مصرف کنندگان ارائه می‌دهد. در چنین ارزیابی فرد یا افرادی به عنوان ارزیاب محصول را جهت منطبق بودن با الزمات امنیتی تحلیل و تست می‌نمایند. براساس این طرح، مرجع مستقل و بی‌طرف یک نهاد دولتی است که مرکز افتا و سازمان فناوری اطلاعات ایفا کننده‌ی آن هستند.

در ادامه این بخش چهار مفهوم در استاندارد ارزیابی معیار مشترک شرح داده شده است:

- پروفایل حفاظتی
- هدف امنیتی
- سند هدف امنیتی
- متدلوژی ارزیابی معیار مشترک

۱,۲ پروفایل حفاظتی

مرکز افتا بر اساس استاندارد ارزیابی معیار مشترک، پروفایل حفاظتی را به صورت مجموعه مستقلی از الزامات امنیتی برای نوعی از محصولات فناوری اطلاعات تعریف نموده، که نیازهای امنیتی مشتری را برآورده می‌نماید. پروفایل حفاظتی در واقع سند طراحی سیستم است که در ابتدا الزامات امنیتی محصول را تعریف و سپس راهکارهای کلی برای برآورده نمودن این دسته از الزامات مشخص نموده است.

در یک پروفایل حفاظتی موارد زیر معرفی می‌شود:

- قابلیت‌های امنیتی ارائه شده در آن نوع از محصولات
- مشخص نمودن نوع انطباقی که یک سند هدف امنیتی می‌تواند نسبت به پروفایل حفاظتی داشته باشد(نوع ادعای انطباق به پروفایل حفاظتی)
- مشخص نمودن بخشی از محصول که موضوع این مجموعه الزامات هستند (تعریف هدف ارزیابی).
- محیطی که موضوعات امنیتی در آن مطرح شده‌اند (محیط عملیاتی).
- مشخص نمودن اهداف امنیتی که در صورت برآورده شدن، قابلیت امنیتی معرفی شده برآورده خواهد شد (اهداف امنیتی).
- مشخص نمودن الزامات امنیتی (الزامات کارکردی، تضمین)
- ارائه دلیلی که نشان می‌دهد الزامات مشخص شده برآورده کننده قابلیت امنیتی تعریف شده می‌باشند.

۲,۲ هدف ارزیابی (محصول)

هدف ارزیابی مجموعه‌ای از نرم‌افزار، میان‌افزار و سخت افزار و همچنین مستندات مربوط به آن است که بر اساس استاندارد ارزیابی معیار مشترک مورد ارزیابی قرار می‌گیرد. هدف ارزیابی، محصول یا بخشی از محصول است که موضوع مجموعه الزامات مشخص شده توسط پروفایل حفاظتی یا سند هدف امنیتی می‌باشد.

۳,۲ سند هدف امنیتی

پروفایل حفاظتی سندی است که به طور مستقل برای نوعی از محصولات تولید می‌شود اما سند هدف امنیتی الزامات امنیتی یک محصول مشخص را برای ارزیابی تحت استاندارد ارزیابی معیار مشترک بیان می‌دارد.
به طورکلی بخش غالبی از سند هدف امنیتی همانند پروفایل حفاظتی بوده و در برگیرنده موارد زیر می‌باشد:

- قابلیت‌های امنیتی ارائه شده در محصول مورد نظر
- مشخص نمودن پروفایل حفاظتی که محصول ادعای انطباق با آن را دارد (ادعای انطباق).
- محیطی که این قابلیت‌ها در آن ارائه شده (محیط عملیاتی)

- اهداف امنیتی که در صورت برآورده شده، قابلیت امنیتی معرفی شده را برآورده خواهد نمود(اهداف امنیتی).
- الزامات امنیتی (الزامات کارکردی، تضمین)
- مشخصات امنیتی هدف ارزیابی

سند هدف امنیتی برگرفته از پروفایل حفاظتی است که به آن ادعای انطباق نموده است. برای اطلاع از جزئیات بیشتر به «راهنمای نوشتن پروفایل حفاظتی/سند هدف امنیتی» مراجعه شود.

۴,۲ متدلوژی ارزیابی معیار مشترک

از آنجا که ممکن است ارزیابی در آزمایشگاه‌های مختلفی انجام شود، نیاز به یک متدلوژی ارزیابی معیار مشترک می‌باشد تا نتایج ارزیابی یک محصول در آزمایشگاه‌های مختلف با هم تفاوتی نداشته باشد. بدین منظور متدلوژی ارزیابی معیار مشترکی ارائه شده که برای هر عنصر تضمین، یک مجموعه از واحدهای کاری را مشخص نموده که باید انجام گیرد. همراه هر واحد کاری ماهیت کار انجام شده شرح داده شده است، برای اطلاع بیشتر به سند CEM از مجموعه اسناد منتشر شده توسط استاندارد ارزیابی معیار مشترک مراجعه شود.

۳ راهنمای تولیدکننده

این بخش راهنمای تولیدکننده در طول فرآیند ارزیابی می‌باشد و در آن وظایف تولید کننده و نیز روابط او با مرکز افتا، سازمان فناوری اطلاعات و آزمایشگاه ارزیابی امنیتی محصول بیان می‌گردد. ارزیابی یک محصول بر اساس طرح ارزیابی امنیتی دارای پنج فاز اصلی می‌باشد که عبارتند از:

فاز اول: آماده‌سازی

هر فعالیتی که پیش از جلسه «نهایی سازی سند هدف امنیتی و شروع ارزیابی» انجام می‌شود.

فاز دوم: ارزیابی اسناد هدف امنیتی

فعالیت‌هایی که در راستای ارزیابی سند هدف امنیتی و دیگر اسناد مورد نیاز انجام می‌گیرد.

فاز سوم: ارزیابی فنی

این فاز پس از ارزیابی کلیه اسناد و آشنایی با محصول به منظور انجام تست‌های عملکردی محصول و ارزیابی آسیب‌پذیری انجام خواهد شد، آزمایشگاه و تولیدکننده جهت رفع اشکالات محصول باید با یکدیگر در تعامل باشند.

فاز چهارم: پایان ارزیابی آزمایشگاه

شروع این فاز با پایان فاز قبلی و برگزاری جلسه «بررسی اعتبارسنجی نهایی» می‌باشد. در این فاز نتایج حاصل از ارزیابی بررسی و در صورت تائید برای محصول گواهی صادر می‌شود.

فاز پنجم: نگهداری و ارزیابی مجدد

فاز پنجم پس از صدور گواهی آغاز می‌شود و فعالیت‌های مربوط به تداوم گواهی و نظارت آن را پیگیری می‌نماید.

۱,۳ فاز اول: آماده‌سازی

وظیفه اصلی تولیدکننده در فاز اول، آماده نمودن بستر مقدماتی برای فرآیند ارزیابی و اعتبارسنجی براساس استاندارد ارزیابی معیار مشترک می‌باشد. تولیدکننده موظف است مستندات و اطلاعات لازم جهت ارزیابی را در اختیار آزمایشگاه قرار دهد، آزمایشگاه نسخه‌ای از این اسناد را در اختیار مرکز افتا قرار می‌دهد. تولیدکننده جهت آگاهی از اطلاعات مورد نیازی که باید جمع‌آوری نماید می‌تواند از آزمایشگاه‌ها یا مراکز خدمات مشاوره کمک گیرد.

اقدامات صورت گرفته در این فاز عبارتند از:

- درخواست ارزیابی محصول از سازمان توسط تولید کننده

تولیدکننده‌ای که در نظر دارد برای محصول خود گواهی امنیتی اخذ نماید باید در ابتدا درخواستی همراه مشخصات محصول برای سازمان فناوری اطلاعات ارسال نماید. فرمت درخواست ارزیابی در سایت سازمان فناوری اطلاعات در دسترس قرار گرفته است.

- تعیین مناسب بودن هدف ارزیابی و تعیین آزمایشگاه توسط مرکز افتا

سازمان پس از دریافت درخواست ارزیابی از تولیدکننده، آن را به منظور بررسی و تعیین آزمایشگاه به مرکز افتا ارجاع می‌دهد. مرکز پس از بررسی درخواست در رابطه با دارا بودن شرایط لازم محصول جهت ارزیابی جمع بندی می‌نماید، در صورت دارا بودن شرایط یک آزمایشگاه در حوزه آن محصول تعیین و به صورت مکتوب به سازمان اعلام می‌نماید، سازمان نیز براساس گزارش مرکز به تولیدکننده معرفی نامه برای آزمایشگاه می‌دهد.

- توافقات و هماهنگی‌های اولیه بین آزمایشگاه و تولید کننده

تولید کننده سپس به آزمایشگاه تعیین شده مراجعه نموده و مراحل زیر را با آزمایشگاه طی می‌کند:

- توافق بر روی روالهای ارتباطی و تعیین افراد رابط از سوی تولید کننده و آزمایشگاه
- توافق بر روی کلیت طرح کاری ارزیابی توسط آزمایشگاه و تولید کننده
- توجیه تولیدکننده در رابطه با روال ارزیابی توسط آزمایشگاه

- منعقد نمودن قرارداد بین آزمایشگاه و تولید کننده

برای انجام امور، قراردادی بین آزمایشگاه و تولید کننده جهت ارزیابی محصول منعقد می‌شود. الزامات مرکز افتا که در قرارداد ارزیابی محصول باید رعایت شوند در ابلاغیه «راهنمای قرارداد ارزیابی امنیتی محصول» آمده است. همچنین جهت اطمینان از تحویل مستندات و موارد لازم جهت ارزیابی محصول توسط تولیدکننده، در قرارداد بین آزمایشگاه و تولیدکننده الزاماتی برای تولید کننده و آزمایشگاه بیان شود. با توجه به حساس بودن و اختصاصی بودن اطلاعات مربوط به محصولات و سامانه‌های فتا و ضرورت در اختیار قرار دادن آنها به آزمایشگاه و مرکز افتا لازم است در قرارداد منعقد شده، قرارداد منع افشاء اطلاعات نیز لحاظ گردد.

- ارائه موارد لازم جهت ارزیابی توسط تولید کننده
  - تهیه سند هدف امنیتی شامل شرح عملکرد محصول و اطلاعات حوزه فیزیکی و منطقی محصول توسط تولید کننده و توافق بر روی آن
  - هدف ارزیابی اعم از سخت‌افزار، نرم‌افزار و میان‌افزار
  - پروفایل حفاظتی
  - مستندات فنی تولید شده در طول توسعه محصول
  - مستندات امنیتی محصول

- ارزیابی اولیه سند هدف امنیتی

پس از آنکه آزمایشگاه مناسب برای ارزیابی محصول تولیدکننده توسط مرکز افتا تعیین شد، و قراردادی بین تولیدکننده و آزمایشگاه جهت ارزیابی محصول منعقد گردید، تولیدکننده باید سند هدف امنیتی را جهت بررسی در اختیار آزمایشگاه قرار دهد تا نسبت به محکم و منسجم بودن آن به عنوان مبنای ارزیابی محصول اطمینان حاصل گردد.

تولیدکننده موظف به رفع و رجوع مسائل و موضوعات برآمده پیرامون سند هدف امنیتی پیش از شروع ارزیابی می‌باشد. آزمایشگاه براساس منابع و اطلاعاتی که در این فاز از تولیدکننده دریافت نموده، امکان موفق بودن یا ناموفق بودن ارزیابی را می‌سنجد، در صورتیکه استنباط شود که ارزیابی می‌تواند با موفقیت

انجام شود، فرآیند ارزیابی را زمانبندی نموده و سند هدف امنیتی را براساس کلاس ASE ارزیابی می‌نماید. پس از اتمام موفق ارزیابی سند، آزمایشگاه آماده‌ی شروع ارزیابی محصول می‌شود.

۱,۱,۳ وظایف تولیدکننده

وظایف تولیدکننده پیش از شروع ارزیابی:

- تعیین نماینده
- منعقد نمودن قرارداد با آزمایشگاه جهت ارزیابی محصول
- هماهنگی با آزمایشگاه جهت تولید و توافق بر روی «طرح کار ارزیابی» و «زمانبندی ارزیابی»
- متعهد شدن به آزمایشگاه جهت ایفای نقش تعریف شده برای تولیدکننده
- تهیه نسخه اولیه سند هدف امنیتی شامل بخش‌های شرح محصول و اطلاعات حوزه فیزیکی و منطقی
- حفظ تمام حقوق قانونی محصول
- شرکت در جلسات آزمایشگاه و مرکز افتا در صورت لزوم

۲,۳ فاز دوم: ارزیابی سند هدف امنیتی

اقدامات صورت گرفته در این فاز عبارتند از:

- آموزش تیم ارزیابی توسط نماینده تولیدکننده

نماینده تولیدکننده باید در طی جلسه‌ای با فراهم نمودن شرایط تست، استفاده از محصول را به تیم ارزیابی آموزش دهد.

- ارائه اسناد مربوطه جهت ارزیابی توسط تولیدکننده

در این فاز تولیدکننده سند کامل هدف امنیتی، سند راهنمای کاربر، سند مشخصات کارکردی، سند تعیین نسخه محصول و سند مدیریت پیکربندی و دیگر اسناد مورد درخواست تیم ارزیابی را تهیه و در اختیار تیم ارزیابی قرار می‌دهد.

- ارزیابی نهایی سند هدف امنیتی و دیگر مستندات

تیم ارزیابی نتایج ارزیابی سند هدف امنیتی و دیگر مستندات (سند راهنمای کاربر، سند مشخصات کارکردی، سند تعیین نسخه محصول، سند مدیریت پیکربندی) را در قالب بسته «بررسی و نهایی سازی سند هدف امنیتی» برای مرکز افتا ارسال می‌نماید. نماینده مرکز افتا مستندات دریافتی را بررسی و در صورت لزوم اقدام به برگزاری جلسه ای برای رفع ابهامات می‌نماید که در آن جلسه نماینده آزمایشگاه و نماینده تولید کننده حضور خواهند داشت.

- بازدید از محل
تیم ارزیابی در صورت لزوم از محل تولیدکننده بازدید به عمل می‌آورد.

- برگزاری جلسه نهایی‌سازی سند هدف امنیتی و شروع ارزیابی
این جلسه با اهداف زیر با حضور نمایندگان مرکز افتا، آزمایشگاه و تولیدکننده برگزار می‌گردد:
  - بررسی و نهایی‌سازی سند هدف امنیتی
  - تعیین نقش و وظایف هر سه بخش و انتظارات آنها
  - توافق بر روی زمانبندی و طرح کار ارزیابی

۱,۲,۳ وظایف تولیدکننده

در طول فاز دوم، مسئولیت‌های تولیدکننده عبارتند از:

- اطلاع رسانی هرگونه تغییر رخ داده در هدف ارزیابی به آزمایشگاه که ممکن است ارزیابی امنیتی را تحت تاثیر قرار دهد.
- پاسخ به هرگونه سوالات آزمایشگاه ناشی از تحلیل سند هدف امنیتی یا دیگر موارد قابل تحویل ارزیابی
- ارائه جزئیات لازم برای حل مشکلات برآمده در طول ارزیابی به آزمایشگاه
- زمانبندی برای تحویل تمام مدارک لازم جهت انجام ارزیابی به آزمایشگاه
- پشتیبانی کارمندان ارزیابی و اعتباربخشی، از جمله آموزش همچنین در دسترس بودن کارمندان تولید کننده محصول برای پاسخ به مباحث فنی

۲,۲,۳ ارتباطات تولیدکننده و آزمایشگاه

آزمایشگاه:

- ارزیابی نمودن مطابق با الزامات قرارداد با تولیدکننده
- فرصت دادن و تعامل با تولیدکننده جهت تصحیح کمبودهای مطرح در سند هدف امنیتی و هدف ارزیابی
- همکاری با مرکز افتا (اعتبارسنج‌ها) در طول ارزیابی
- ارسال گزارش مشاهدات در صورت لزوم
- تولید گزارش فنی ارزیابی و دیگر مستندات
- تسهیل جریان اطلاعات بین تولیدکننده و مرکز افتا
- آگاهی کامل از تفاسیر فعالیت‌های تضمین و استاندارد ارزیابی معیار مشترک و روال‌ها و خط‌مشی‌های تاثیرگذار بر روی ارزیابی

۳,۲,۳ ارتباطات تولیدکننده و اعتبارسنج

نماینده مرکز افتا (اعتبارسنج):

- همکاری با آزمایشگاه
- ارسال تصمیمات به موقع در رابطه با گزارش مشاهدات تولید شده توسط آزمایشگاه
- آگاهی کامل از روال‌ها و خط‌مشی‌های استاندارد ارزیابی معیار مشترک و مرکز افتا و تکنولوژی که مورد ارزیابی قرار گرفته

۳,۳ فاز سوم: ارزیابی فنی

فاز سوم پس از پایان جلسه «شروع ارزیابی و بررسی و نهایی سازی سند هدف امنیتی» آغاز می‌گردد و شامل دو بخش «روش تست محصول» و «روش تحلیل آسیب‌پذیری» می‌باشد. آزمایشگاه و تولیدکننده در حین این فاز باید جهت رفع اشکالات با یکدیگر در تعامل باشند و رونوشتی از تبادلات توسط آزمایشگاه برای مرکز افتا ارسال گردد. برای اطلاع ازجزئیات این فاز به سند «راهنمای آزمایشگاه» مراجعه شود.

۴,۳ فاز چهارم: پایان ارزیابی آزمایشگاه

در این فاز آزمایشگاه تمام مستندات ارزیابی را به نماینده مرکز افتا تحویل می‌دهد پس از بررسی این مستندات توسط نماینده مرکز افتا جلسه‌ای با هدف بررسی نتایج تست و با حضور نمایندگان مرکز افتا، آزمایشگاه و تولیدکننده برگزار می‌شود در این جلسه ممکن است ازسوی مرکز افتا کارشناسان خبره در حوزه محصول نیز شرکت نمایند. در صورت موفقیت آمیز بودن این جلسه، در پایان آزمایشگاه نسخه پیشنویس «گزارش صدور گواهی» را تهیه و برای مرکز افتا ارسال می‌نماید، پس از بررسی این گزارش سرپرست مرکز افتا تصمیم‌گیری می‌نماید که:

- ارزیابی با موفقیت انجام شده است

  مرکز افتا موفقیت آمیز بودن ارزیابی را به اطلاع سازمان فناوری اطلاعات می‌رساند و سازمان گواهی محصول را صادر می‌نماید و نام و مشخصات محصول را در لیست محصولات تائید شده در سایت سازمان قرار می‌دهد.
- ارزیابی ناموفق بوده است

  مرکز افتا، آزمایشگاه و تولیدکننده را از تکمیل ناموفق ارزیابی و علت این تصمیم‌گیری به صورت مکتوب مطلع می‌نماید.

۱,۴,۳ اعتبار گواهی

گواهی صادر شده برای محصول از تاریخ صدور گواهی به مدت دو سال اعتبار دارد. شرایطی که سبب لغو گواهی خواهند شد، عبارتند از:

- مرکز گواهی تشخیص دهد که محصول معیارهای برای معتبر بودنش را رعایت نمی‌کند.
- تولیدکننده محصول دارای گواهی، شرایط استفاده از آن را نقض می‌کند.
- عدم ارسال سالیانه گزارش «تحلیل آسیب‌پذیری» توسط تولیدکننده

۲,۴,۳ مدیریت رکوردهای ارزیابی

تمام رکوردهای ارزیابی و هرآنچه که در ارتباط با هر ارزیابی آماده شده، براساس طرح ارزیابی امنیتی برای مدت پنج سال پس از تکمیل ارزیابی نگهداری می‌شود. پس از منقضی شدن دوره آرشیو، تمام رکوردهای غیر اختصاصی حذف می‌شوند.

۵,۳ فاز پنجم: نگهداری و ارزیابی مجدد

فاز پنجم پس از صدور گواهی آغاز می‌شود و فعالیت‌های مربوط به تداوم گواهی و نظارت آن را پیگیری می‌نماید. مرکز افتا به تولیدکننده‌ی محصول این فرصت را می‌دهد تا نتایج ارزیابی قبلی را ارتقاء دهد و هر زمانی با هزینه معقول امکان شرکت در ارزیابی و اعتبارسنجی را داشته باشد. روال‌های نگهداری از گواهی در سند «تداوم تضمین: راهنمای نگهداری و ارزیابی مجدد» آمده است.

۱,۵,۳ درخواست تداوم گواهی

در صورتیکه محصول ارزیابی شده پس از صدور گواهینامه دستخوش تغییراتی گردد و تولید کننده خواهان تداوم اعتبار گواهی خود باشد، باید درخواستی برای تداوم اطمینان محصول همراه با «گزارش تحلیل اثر تغییرات» به مرکز افتا ارسال نماید.

مرکز افتا با بررسی این گزارش تصمیم می‌گیرد که محصول مجدداً ارزیابی گردد یا تضمین محصول حفظ شود. در صورتیکه اثر تغییرات که در این گزارش آمده بر روی امنیت محصول اندک باشد، پروسه تداوم گواهی محصول اجرا خواهد شد. در صورتیکه تغییرات گزارش شده اثر عمده‌ای بر روی امنیت محصول داشته باشند، محصول باید مجدداً ارزیابی شود.

۲,۵,۳ گزارش سالانه تحلیل آسیب‌پذیری

تولید کننده هر ساله باید گزارش تحلیل آسیب پذیری برای محصول خود را به مرکز افتا ارسال نماید. مرکز افتا در صورت لزوم این گزارش را برای دریافت نظر به آزمایشگاه ارزیابی کننده محصول ارسال می‌نماید. در صورت

کامل بودن گزارش و عدم نیاز به ارزیابی مجدد، اعتبار گواهی آن محصول یکسال دیگر تمدید می‌شود. در صورتی که مرکز تشخیص دهد گزارش ناقص است و یا آسیب پذیری جدیدی آن محصول را تهدید می‌نماید، پس از تعامل با تولید کننده تصمیم به انجام ارزیابی مجدد، تمدید گواهی و یا تعلیق گواهی خواهد گرفت.

خط‌مشی استفاده از لوگوی گواهی در پیوست الف شرح داده شده است.

۳,۵,۳ وظایف تولیدکننده

در طول فاز پنجم از تولیدکننده انتظار می‌رود:

- مرکز افتا را از هرگونه عامل احتمالی که سبب نامعتبر شدن گواهی می‌گردد، آگاه نماید.
- تبلیغ و فروش محصول براساس گواهی استاندارد ارزیابی معیار مشترک معتبر
- اطمینان از نگهداری گواهی با کنترل نمودن تغییرات صورت گرفته در سند هدف امنیتی، گزارش فنی ارزیابی یا گزارش اعتبارسنجی برای تغییراتی که در هدف ارزیابی رخ می‌دهد.
- حفظ و نگهداری تمام اطلاعات تغییریافته و مدارک تست مربوطه برای استفاده بالقوه در ارزیابی‌های آینده

پیوست الف

لوگوی گواهی استاندارد ارزیابی معیار مشترک توسط فروشندگان جهت فروش و تبلیغات «محصول منطبق بر استاندارد» استفاده می‌شود. اصطلاح محصول منطبق بر استاندارد تنها به محصولاتی اطلاق می‌گردد که ارزیابی آنها مطابق روال‌های مرکز افتا با موفقیت به پایان رسیده و توسط مرکز افتا و سازمان فناوری اطلاعات برای آن گواهی صادر شده و در لیست محصول معتبر در سایت سازمان قرار گرفته است.

استفاده‌های بالقوه از لوگوی گواهی

- **محصولات و بسته بندی آن**

از لوگوی گواهی ممکن است بر روی محصول و بسته‌بندی آن استفاده گردد.

- **بروشور/سایت**

لوگوی گواهی توسط فروشندگان در بازاریابی/بروشورهای فروش و وب سایت‌ها استفاده می‌گردد. در صورتیکه از لوگو در بالا یا پائین صفحه استفاده شود، تمام متن و تصاویر در آن صفحه تنها باید به محصول منطبق بر استاندارد اشاره داشته باشد.

در صورتیکه از لوگو در کنار یک پاراگراف خاص استفاده شود، تمام متن و تصاویر در آن پاراگراف تنها باید به محصول منطبق بر استاندارد اشاره داشته باشد.

لازم به ذکر است که در هر حال باید به شماره نسخه محصول نیز عنوان گردد.

- **علائم تجاری**

تنها محصول منطبق بر استاندارد (محصول واقعی، ماکت یا تصویر) ممکن است در کنار لوگوی گواهی نمایش داده شود.