به نام خدا

پروفایل حفاظتی
برنامه‌های کاربردی تحت شبکه

مهر ۹۵

نسخه ۱,۰

فهرست

۱ مقدمه ۵
۲ اصطلاحات ۵
۳ شرح محصول ۶
۳,۱ مؤلفه‌های محیط عملیاتی ۸
۳,۲ انواع کاربران ۱۱
۳,۳ ویژگیهای امنیتی محصول ۱۱
۴ مسائل امنیتی ۱۳
۴,۱ تهدیدات ۱۳
۴,۲ خطمشی امنیتی ۱۵
۴,۳ فرضیات ۱۶
۵ اهداف امنیتی ۱۷
۵,۱ اهداف امنیتی برای محصول ۱۷
۵,۲ اهداف امنیتی برای محیط عملیاتی ۲۰
۶ الزامات کارکرد امنیتی ۲۱
۶,۱ کلاس ممیزی امنیت ۲۶
۶,۲ کلاس پشتیبانی از رمزنگاری ۳۶

۶,۳ کلاس شناسایی و احراز هویت ۳۷
۶,۴ کلاس حفاظت از داده‌های کاربری ۴۵
۶,۵ کلاس مدیریت امنیت ۵۴
۶,۶ کلاس حفاظت از توابع امنیتی محصول ۶۰
۶,۷ کلاس دسترسی به محصول ۶۵
۶,۸ کلاس تخصیص منابع ۶۹
۶,۹ کلاس کانال‌ها/مسیرهای مورد اعتماد ۶۹
۷ الزامات تضمین امنیت ۷۱
۷,۱ کلاس توسعه ۷۲
۷,۲ کلاس راهنمای کاربر ۷۵
۷,۲,۱ راهنمای کاربردی ۷۵
۷,۲,۲ راهنمای آماده‌سازی ۷۸
۷,۳ کلاس آزمون ۸۰
۷,۳,۱ آزمون مستقل ۸۰
۷,۴ کلاس آسیب‌پذیری ۸۲
۷,۴,۱ تحلیل آسیب‌پذیری ۸۲
۷,۵ کلاس پشتیبانی از چرخه حیات ۸۴
۷,۵,۱ قابلیت‌های پیکربندی ۸۴

۷,۵,۲ حوزه پیکربندی ۸۵
۸ پیوست یک:: الزامات کلاس پشتیبانی از رمزنگاری مبتنی بر انتخاب ۸۶
۹ پیوست دو: الزامات پروتکل TLS مبتنی بر انتخاب ۸۹
۱۰ پیوست سه: الزامات کلاس ممیزی مبتنی بر انتخاب ۹۲

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه نموده است. این پروفایل حفاظتی، به بیان الزامات برنامه کاربردی تحت شبکه می‌پردازد.

۲ اصطلاحات

مستند: به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات و فعالیت‌های سازمانی مورداستفاده قرار می‌گیرند، مستند گفته می‌شود.

رکورد: مستندی که اطلاعات فعالیت‌ها، رویدادها و نتایج حاصله را نگهداری می‌کند؛ به عبارت دیگر یک رکورد مستندی است که مدرک انجام یک فعالیتی مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

رکورد ممیزی: رکوردی که حاوی اطلاعات رویدادهایی است که برای ممیزی برنامه کاربردی تحت شبکه موردنیاز است و در محل ذخیره‌سازی ممیزی، ذخیره می‌شود.

داده‌های کاربری ذخیره‌شده: فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل مستندات تولیدشده با استفاده از برنامه کاربردی Microsoft Office، نامه‌های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.

موجودیت فعال: موجودیتی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون مدیر، کاربر نهایی و غیره.

موجودیت غیرفعال: موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌نماید و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایل‌ها توسط مهاجم. (رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.)

مشخصه‌های موجودیت فعال: مشخصه‌های هر موجودیت فعال می‌تواند از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر باشد.

مشخصه‌های موجودیت غیرفعال: مشخصه‌های هر موجودیت غیرفعال می‌تواند از قبیل نوع، نام و اندازه مستند باشد.

۳ شرح محصول

محصول مورد ارزیابی، برنامه کاربردی مبتنی بر شبکه است که برای مدیریت رکوردها و مستندات مورداستفاده قرار می‌گیرد. از جمله وظایف این برنامه‌های کاربردی می‌توان به جمع‌آوری، ذخیره و توزیع مستندات، پیام‌ها و فرم‌های ارتباطات اداری بین افراد اشاره نمود.

به‌طور کلی برنامه کاربردی تحت شبکه برای رکوردها و مستندات الکترونیکی از فعالیت‌های زیر استفاده می‌کند:

- ثبت رکوردهای الکترونیکی
- مدیریت گردش کار رکوردهای الکترونیکی
- ایجاد و مدیریت فرآیندهای آرشیو
- انجام امور جستجو و گزارش دهی
- قابلیت مدیریت کاربران
- پشتیبانی از سازوکارهای امن‌سازی ارتباطات
- سازوکارهای احراز هویت و کنترل دسترسی

محصول اعمال فوق را با کمک مؤلفه‌های نشان داده‌شده در شکل ۱ انجام می‌دهد.

شکل ۱: مؤلفه‌های برنامه کاربردی تحت شبکه

۳,۱ مؤلفه‌های محیط عملیاتی

یک برنامه کاربردی تحت شبکه، یک برنامه اجرایی بر روی بستر شبکه است و با مؤلفه‌های شبکه در تعامل است که بر روی سیستم‌عامل اجرایی در محیط شبکه اجرا می‌گردد. محصول با واحد/واحدهای ذخیره‌سازی به‌منظور نگهداری رکوردها و با مؤلفه‌های ممیزی به‌منظور نگهداری رکوردهای ممیزی در تعامل است؛ در ادامه، این مؤلفه‌ها با جزئیات شرح داده می‌شوند.

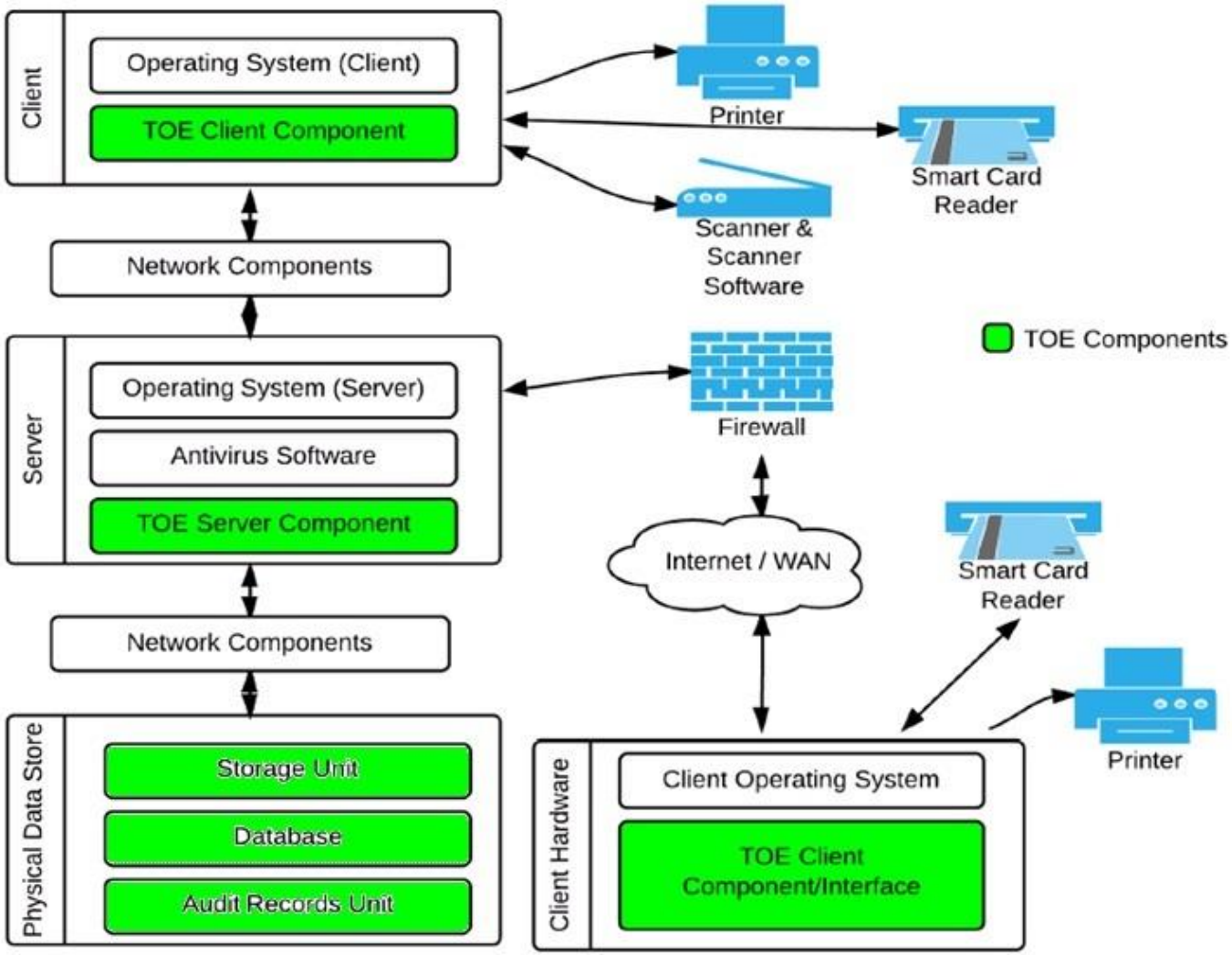
محیط عملیاتی محصول شامل مؤلفه‌های نرم‌افزاری و سخت‌افزاری و همچنین ویژگی‌های کارکردی و امنیتی اصلی است که در این سند پوشش داده‌شده‌اند. شکل ۲ بیانگر سخت‌افزار و نرم‌افزارهایی است که محصول با آن‌ها در تعامل است، این شکل چگونگی تعاملات محصول با محیط عملیاتی را نمایش می‌دهد:

سرور: سرور مؤلفه سخت‌افزاری است که مؤلفه سروری محصول بر روی آن اجرا می‌گردد. سرور می‌تواند به‌صورت فیزیکی یا مجازی باشد، در هر دو حالت امنیت سرور به امنیت محصول بستگی دارد. پیکربندی و قابلیت‌های سرور می‌تواند با توجه به تعداد کاربران، تعداد اتصالات و غیره متفاوت باشد.

سیستم کاربر: سخت‌افزار و سیستم‌عاملی است که به کاربران اجازه دسترسی به محصول را می‌دهد. این مؤلفه معمولاً یک کامپیوتر بوده ولی می‌تواند یک تبلت یا گوشی هوشمند نیز باشد، در این پروفایل حفاظتی فرض شده که کلاینت یک کامپیوتر است. دو نوع کلاینت وجود دارد. یکی برای کاربر پایانی و نوع دیگر برای کاربرانی که رکوردها و مستندات را به داخل محصول وارد می‌نمایند. اتصالات بین کلاینت‌ها و مؤلفه‌های مرکزی محصول می‌تواند به‌صورت اینترنت، اینترانت یا VPN باشد.

سیستم‌عامل: محصول بر روی یک سیستم‌عامل اجرا می‌شود و ارتباطات بین محصول و واحد ذخیره‌سازی، واحد رکوردهای ممیزی، مؤلفه‌های شبکه و سرور توسط سیستم‌عامل ارائه می‌شود.

مؤلفه‌های شبکه: محصول به‌واسطه سیستم‌عامل و سرور با مؤلفه‌های شبکه در تعامل است. لازم است اتصالات شبکه بین کلاینت‌ها و سرور محصول به‌صورت امن باشد. کلاینت محصول قادر به انجام اقداماتی همانند چاپ، اسکن و غیره است. اتصالات بین این مؤلفه‌ها و سرور معمولاً به‌صورت یک شبکه محلی است.



شکل ۲: محیط عملیاتی محصول

فایروال: دسترسی اینترانت به‌وسیله‌ی این مؤلفه امن می‌گردد.

نرم‌افزار آنتی‌ویروس: نرم‌افزار آنتی‌ویروس جهت بررسی مستندات و رکوردهای ورودی مورداستفاده قرار می‌گیرد.

پایگاه داده: محصول با یک پایگاه داده برای حفظ و نگهداری داده‌های خود در تعامل نزدیک است. رکوردها و مستندات می‌توانند در پایگاه داده یا به‌صورت مجزا حفظ و نگهداری شوند. در زمان نیاز به یک مجموعه داده خاص، یک درخواست به پایگاه داده ارسال و نتایج آن گرفته می‌شود.

واحد ذخیره‌سازی مستندات و رکوردها: رکوردها و مستندات می‌توانند به‌صورت مجزا در سمت سروری که محصول بر روی آن اجرا می‌گردد باقی مانده تا محصول به‌آسانی تحت تأثیر آسیب‌پذیری امنیتی بالقوه در واحد ذخیره‌سازی قرار نگیرد.

واحد ذخیره رکوردهای ممیزی: همانند واحدهای ذخیره‌سازی، واحد رکوردهای ممیزی در سمت سروری قرار می‌گیرد که محصول بر روی آن اجرا می‌گردد. این واحد می‌تواند به‌صورت مؤلفه مجزا و یا بخشی از واحد ذخیره‌سازی باشد.

کارت‌خوان هوشمند: کارت‌خوان یک مؤلفه سخت‌افزاری است که دارای گواهی مورد اعتماد است و برای امضاء اسناد الکترونیکی مورداستفاده قرار می‌گیرد. در حال حاضر رایج‌ترین نوع کارت‌خوان توکن USB است. از آنجائی که این مؤلفه مبتنی بر سخت‌افزار بوده و به شبکه متصل نیست، سطح بالایی از امنیت را فراهم می‌نماید. از این‌رو می‌تواند برای احراز هویت مورداستفاده قرار گیرد.

اسکنر و درایور آن: کاربرانی که برای اسکن نمودن مجاز هستند، رکوردها و مستنداتی که به شکل کاغذی دریافت می‌کنند را اسکن می‌نماید.

پرینتر: مؤلفه‌ای است که به کاربران محصول مطابق با مجوز کاربر، اجازه چاپ هر رکورد یا مستندی را می‌دهند.

۳,۲ انواع کاربران

حداقل دو دسته کاربر برای محصول وجود دارد:

- کاربر عادی

- مدیر سیستم

علاوه بر نقش‌های لیست شده در بالا، محصول ممکن است دارای نقش‌های دیگری نیز باشد. در صورت وجود نقش‌های دیگر لازم است در سند هدف امنیتی ذکر گردد.

کاربر عادی: کاربر عادی از محصول به‌صورت یک جعبه سیاه استفاده می‌نماید و نیز قادر به مدیریت داده‌های تحت مالکیتش است. کاربر عادی در صورت داشتن مجوز می‌تواند رکوردها و مستندات را جستجو، لیست و مشاهده نماید. علاوه بر آن کاربر عادی می‌تواند سند یا رکورد جدیدی ایجاد نماید یا سند و رکوردی که مالک آن است را حذف نماید. این نوع کاربر می‌تواند مستندات را بایگانی نماید و باید قادر به دسترسی اسناد بایگانی‌شده خود باشد.

مدیر سیستم: مدیر، دارای مجوز خاص برای مدیریت محصول است. مدیر سیستم می‌تواند یک نفر باشد یا برای بخش‌های مختلف محصول مدیران مختلفی وجود داشته باشد، همانند مدیر پایگاه داده، مدیر شبکه، مدیر برنامه کاربردی و غیره. همچنین مدیر دارای سطح دسترسی کامل برای دسترسی به برنامه کاربردی، پایگاه داده، فایل سیستم و دیگر موجودیت‌ها است.

۳,۳ ویژگی‌های امنیتی محصول

احراز هویت و مجوزدهی: عملیات احراز هویت و مجوزدهی باید به‌طور مؤثری انجام شود. احراز هویت به‌طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌گیرد. لازم به ذکر است برای مدیریت کلمه عبورهای مورداستفاده باید روال‌های امن وجود داشته باشد. در صورتی که محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احراز هویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می‌شود. از جمله سازوکارهای احراز هویت می‌توان به وارسی نام کاربری و کلمه عبور، وارسی SMS، احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، وارسی بیومتریک و توکن سخت‌افزاری اشاره نمود.

کنترل دسترسی: محصول، قابلیت‌های لازم برای محدود کردن دسترسی را دارد، به‌طوری که تنها موجودیت‌های مجاز، دارای دسترسی به داده و کارکردهای محصول هستند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌گیرد. محصول ممکن است همچنین آدرس‌های IP اتصالات فعال را کنترل نماید و تنها به آدرس‌های IP از پیش تعریف‌شده در یک بازه زمانی خاص برای عملیات حساس اجازه اتصال دهد.

ممیزی: محصول به‌صورت خودکار، رکوردهای ممیزی را به‌منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی‌ها، تغییرات کنترل دسترسی و پیکربندی جمع‌آوری می‌نماید. محتوای رکوردهای ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکوردهای ممیزی را ندارند.

مدیریت: محصول، برای مدیریت کاربران و دسترسی‌ها واسطهای مدیریتی لازم را فراهم می‌نماید. سرعت و دقت این واسطها در تصمیم‌گیری در طول یک رخداد امنیتی بسیار مهم است.

صحت رکوردها و بررسی منابع: حذف یا تغییر هر رکورد توسط محصول مجاز نیست؛ بنابراین، دسترسی و تغییر سند و/یا فراداده[۱] آن باید محدود گردد. صحت رکوردهای ذخیره‌شده، توسط روشی مانند امضای دیجیتال مهیا می‌گردد.

پشتیبان‌گیری: عملیات پشتیبان‌گیری بر روی داده، مستندات و رکوردهای ممیزی که محصول از آن‌ها محافظت می‌نماید، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

کنترل گردش مستندات و اطلاعات: حداکثر اندازه فایل می‌تواند به‌صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره‌سازی را در نظر گرفته و در برابر سرریز ذخیره‌سازی اقدامات احتیاطی لازم را اتخاذ می‌نماید. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

درهم‌سازی/رمز نمودن داده حساس: مثالی از داده حساس کلمه‌های عبور یا رکوردهای محرمانه است. داده حساس بر روی محصول به‌صورت واضح ذخیره نمی‌شوند و با سازوکاری از آن‌ها حفاظت می‌شود. همچنین باید رکوردهای محرمانه به‌صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهم‌سازی و رمزنگاری انتخاب‌شده باید به‌اندازه کافی قوی باشد طوری که توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

---

[۱] MetaData

۴ مسائل امنیتی

۴,۱ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم می‌تواند با سود بردن از نقض‌های امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم می‌تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجادشده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و داده‌های حفاظت‌شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت‌شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین‌شده نیست. مهاجم ممکن است درصدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول است تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از

تهدیدات	توضیحات
	رکوردهای ممیزی جلوگیری کند (به‌عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشای اطلاعات	داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور واردکننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می‌تواند سبب گردد محصول در یک بازه زمانی غیرقابل‌دسترسی یا بدون استفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص است که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDoS است که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده‌های ورودی مخرب	مهاجم می‌تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم می‌تواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.
شنود شبکه	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده‌های ردوبدل شده بین محصول و یک یا چند کاربر

تهدیدات	توضیحات
	از راه دور و یا محلی است. به‌عنوان مثال می‌توان به موردی اشاره کرد که در آن یک کاربر تلاش می‌کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می‌نماید.

۴,۲ خط‌مشی امنیتی

خط‌مشی‌ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت‌شده هستند و معمولاً به‌منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می‌گیرند.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مؤلفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوری که مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورداستفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش‌فرض، خطاهای پیش‌فرض و صفحات 404، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خط‌مشی سازمانی بسیار مهم است به‌خصوص زمانی که محصول یا هر مؤلفه تعاملی به‌طور گسترده مورداستفاده قرار می‌گیرد؛ بنابراین با تضمین نمودن منحصربه‌فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورداستفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۴,۳ فرضیات

فرضیات	توضیحات
کاربران آموزش‌دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه‌نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند.
توسعه‌دهندگان مجرب	فرض شده است تمام کارمندان توسعه‌دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته‌شده را اتخاذ می‌نمایند.
محیط امن	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته‌شده است. فرض شده است که دسترسی به محیط کاری محصول به‌طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ‌شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیرقانونی از محصول به‌دست‌آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت می‌گیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجادشده یا واردشده توسط محصول، واحد ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند و بنا بر وجود نسخه پشتیبان هیچ داده‌ای از دست نمی‌رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی‌دهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورداستفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به‌طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.

فرضیات	توضیحات
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذشده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.
انکار سرویس توزیع‌شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به‌موقع از رخداد امنیتی بحرانی آگاه نماید.

هدف امنیتی	توضیحات
احراز هویت	محصول باید هر کاربری را تعریف نموده و آن‌ها را به‌طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوری که کاربران را ملزم به استفاده از کلمه‌های عبور قدرتمند نماید. محصول باید اجازه طبقه‌بندی رکوردها و مستندات را دهد و با توجه به طبقه‌بندی آن‌ها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصول باید برای کاربران به‌صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قوی‌تری مدیر سیستم را احراز هویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت بر اساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف‌شده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.

هدف امنیتی	توضیحات
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارآمد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط‌های مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش‌های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش‌ها و مجوزهایی تنظیم نماید.
مدیریت خطا	محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ‌داده در طول عملیات محصول باید به کاربر به‌صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ‌داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده‌های باقیمانده	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل‌دسترس می‌گردد.
ارتباطات امن مبتنی برTLS	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۵,۲ اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی محیطی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مؤلفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به‌طور مناسب در قبال هر حمله DoS یا DDoS محافظت‌شده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده‌شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.
کاربران آموزش‌دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده‌کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه‌دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه‌دهنده‌ی محصول در زمینه امنیت تجربه داشته و آن‌ها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته‌شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول است. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده‌شده به‌منظور آزمودن باید پاک یا غیرقابل‌دسترس گردند.

اهداف امنیتی محیطی	توضیحات
پشتیبان‌گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال‌های از پیش تعریف‌شده استفاده گردد. همچنین باید از واحدهای ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده‌شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲	**تولید داده ممیزی ۲**	FAU_GEN.1.2
۳	**تولید داده ممیزی ۳**	FAU_GEN.2.1
۴	**بازبینی داده ممیزی ۱**	FAU_SAR.1.1
۵	**بازبینی داده ممیزی ۲**	FAU_SAR.1.2
۶	**بازبینی داده ممیزی ۳**	FAU_SAR.2.1
۷	**بازبینی داده ممیزی ۴**	FAU_SAR.3.1
۸	**ذخیره‌سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۹	**ذخیره‌سازی رویدادهای ممیزی ۲**	FAU_STG.1.2
۱۰	**ذخیره‌سازی رویدادهای ممیزی ۶**	FAU_STG.3.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱	**ذخیره‌سازی رویدادهای ممیزی ۷**	FAU_STG.4.1
۱۲	**انتخاب داده ممیزی ۱**	FAU_SEL.1.1
۱۳	**عملیات رمزنگاری ۱(۱)**	FCS_COP.1.1(1)
۱۴	**عملیات رمزنگاری ۱ (۲)**	FCS_COP.1.1(2)
۱۵	**مدیریت کلمه عبور**	FIA_PMG_EXT.1.1
۱۶	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
۱۷	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
۱۸	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۱۹	**شناسایی کاربر ۱**	FIA_UID.1.1
۲۰	**شناسایی کاربر ۲**	FIA_UID.1.2
۲۱	**احراز هویت کاربر ۱**	FIA_UAU.1.1
۲۲	**احراز هویت کاربر ۲**	FIA_UAU.1.2
۲۳	**احراز هویت کاربر ۷**	FIA_UAU.5.1
۲۴	**احراز هویت کاربر ۸**	FIA_UAU.5.۲
۲۵	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**	FIA_USB.1.1
۲۶	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**	FIA_USB.1.2
۲۷	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**	FIA_USB.1.۳
۲۸	**حفاظت از اطلاعات باقیمانده در منابع ۲**	FDP_RIP.2.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۹	**ورود داده‌های کاربری به محصول ۴**	FDP_ITC.2.1
۳۰	**ورود داده‌های کاربری به محصول ۵**	FDP_ITC.2.2
۳۱	**ورود داده‌های کاربری به محصول ۶**	FDP_ITC.2.3
۳۲	**ورود داده‌های کاربری به محصول ۷**	FDP_ITC.2.۴
۳۳	**ورود داده‌های کاربری به محصول ۸**	FDP_ITC.2.۵
۳۴	**خروج داده‌های کاربری از محصول ۳**	FDP_ETC.2.1
۳۵	**خروج داده‌های کاربری از محصول ۴**	FDP_ETC.2.۲
۳۶	**خروج داده‌های کاربری از محصول ۵**	FDP_ETC.2.۳
۳۷	**خروج داده‌های کاربری از محصول ۶**	FDP_ETC.2.۴
۳۸	**صحت داده‌های کاربری ذخیره‌شده ۲**	FDP_SDI.2.1
۳۹	**صحت داده‌های کاربری ذخیره‌شده ۳**	FDP_SDI.2.2
۴۰	**خط‌مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۴۱	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۴۲	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۴۳	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۴۴	**عملیات کنترل دسترسی ۴**	FDP_ACF.1.۴
۴۵	**مدیریت کارکرد در محصول ۱**	FMT_MOF.1.1
۴۶	**مدیریت مشخصه‌های امنیتی ۱**	FMT_MSA.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۷	مدیریت مشخصه‌های امنیتی ۳	FMT_MSA.3.1
۴۸	مدیریت مشخصه‌های امنیتی ۴	FMT_MSA.3.2
۴۹	مدیریت داده‌های محصول ۱-مدیر سیستم	FMT_MTD.1.1(1)
۵۰	مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	FMT_MTD.1.1(2)
۵۱	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۵۲	نقش‌های امنیتی ۱	FMT_SMR.1.1
۵۳	نقش‌های امنیتی ۲	FMT_SMR.1.2
۵۴	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۵۵	سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۵۶	سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.1.۲
۵۷	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۵۸	مهرهای زمانی ۱	FPT_STM.1.1
۵۹	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۶۰	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۶۱	محدودیت بر روی چندین نشست هم‌زمان ۱	FTA_MCS.1.1
۶۲	محدودیت بر روی چندین نشست هم‌زمان ۲	FTA_MCS.1.2
۶۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۶۴	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۵	**سوابق دسترسی به محصول ۱**	FTA_TAH.1.1
۶۶	**سوابق دسترسی به محصول ۲**	FTA_TAH.1.۲
۶۷	**سوابق دسترسی به محصول ۳**	FTA_TAH.1.۳
۶۸	**برقراری نشست ۱**	FTA_TSE.1.1
۶۹	**تحمل خطا ۱**	FRU_FLT.1.1
۷۰	**مسیر امن ۱**	FTP_TRP.1.1
۷۱	**مسیر امن ۲**	FTP_TRP.1.2
۷۲	**مسیر امن ۳**	FTP_TRP.1.3
الزامات پیوست یک		
۷۳	**مدیریت کلید رمزنگاری ۱**	FCS_CKM.۱.۱
۷۴	**مدیریت کلید رمزنگاری ۴**	FCS_CKM.۴.۱
۷۵	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۳)**	FCS_COP.۱.۱(۳)
۷۶	**عملیات رمزنگاری ۱ (۴)**	FCS_COP.۱.۱(۴)
الزامات پیوست دو		
۷۷	**الزامات پروتکل TLS Server/ احراز هویت ۱**	FCS_TLSS_EXT.1.1
۷۸	**الزامات پروتکل TLS Server/ احراز هویت ۲**	FCS_TLSS_EXT.1.2
۷۹	**الزامات پروتکل TLS Server/ احراز هویت ۳**	FCS_TLSS_EXT.1.3
الزامات پیوست سه		

۶,۱ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**

محصول باید بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:

- آغاز و اتمام توابع ممیزی؛
- تمامی رویدادهای قابل ممیزی که در جدول زیر آمده است و

مؤلفه	رویداد قابل ممیزی	جزئیات
بازبینی داده ممیزی ۳	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
صحت داده‌های کاربری ذخیره‌شده ۲	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
احراز هویت کاربر ۱	ثبت کاربرد ناموفق از سازوکار احراز هویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
احراز هویت کاربر ۷	ثبت نتایج احراز هویت (حداقل)	

	ثبت هر سازوکار احراز هویت فعال همراه با نتیجه نهائی (پایه)	
شناسایی کاربر ۱	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبدأ، شناسایی نقطه پایانی اتصال
مدیریت کلمه عبور	ثبت رد هر کلمه عبور آزمون شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
مدیریت مشخصه‌های امنیتی ۱	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	
مدیریت داده‌های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به‌خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به‌خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
حفظ وضعیت امن در زمان شکست ۱	ثبت شکست در محصول (پایه)	
تحمل خطا ۱	ثبت هر شکست شناسایی‌شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست است (پایه)	
برقراری نشست ۱	ثبت منع آغاز نشست به دلیل سازوکار آغاز نشست (حداقل) ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه)	

- [انتخاب: رویدادهای قابل ممیزی در سطح پایه (این رویدادها در «پیوست سه» آمده است)]،

- [اختصاص: دیگر رویدادهای ممیزی برای کارکردهای مدیریتی محصول]

نکته کاربردی ۱:

گروهی از رویدادهای ممیزی دیگر را بر اساس الزامات اختیاری و انتخابی برگرفته‌شده از «پیوست سه» به محصول مورد ارزیابی اضافه شوند؛ بنابراین، نویسنده سند هدف امنیتی الزامات مرتبط از «پیوست سه» را انتخاب نموده و به‌صورت تکمیل‌شده در سند بیان نماید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول[۲]**

توسعه‌گر محصول باید قالب و نحوه ذخیره‌سازی رکوردهای ممیزی را در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بیان نماید و چگونگی استخراج رکوردهای ممیزی توسط مدیر سیستم و یا ارزیاب به‌منظور تحلیل داده‌ها، توضیح داده شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نماید تا نسبت به ارائه فهرستی از رویدادهای قابل ممیزی در محل ذخیره‌سازی به شکل مناسب و قابل‌درک اطمینان حاصل نماید.

- **آزمون‌ها**

ارزیاب باید آزمون‌های زیر را برای هر کدام از انواع رویدادها انجام دهد:

آزمون اول: ارزیاب باید نشستی را با سرور ایجاد و درخواستی به آن ارسال نماید. سپس باید تولید لاگ در سرور برای درخواست ارسال‌شده را بررسی نماید.

آزمون دوم: ارزیاب باید عملیاتی را انجام دهد که منجر به ثبت هر کدام از رویدادهای قابل ممیزی می‌شود. سپس ثبت و یا عدم ثبت آن‌ها را بررسی نماید.

آزمون سوم: ارزیاب باید با انجام یک عمل غیرمجاز، عدم تولید لاگ در سرور را بررسی نماید.

[۲] TOE Summory Specification (TSS)

۲	**تولید داده ممیزی ۲**
محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: • تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد • [اختصاص: هر نوع اطلاعات قابل ممیزی دیگر.] **اقدامات ارزیابی:** • **سند راهنمای محصول** ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید در سند مذکور، نحوه نمایش لاگ‌های ممیزی ذخیره‌شده در شکل و فرمت مناسب شرح داده‌شده است. • **آزمون‌ها** ارزیاب باید بررسی کند برای لاگ ثبت‌شده در سرور، اطلاعات ذکرشده در این الزام وجود دارد یا خیر.	
۳	**تولید داده ممیزی ۳**
برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی‌شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است را شناسایی و ثبت نماید. **اقدامات ارزیابی:** • **بخش خلاصه مشخصات محصول** در این بخش باید در صورت امکان روش‌هایی که باعث عدم انقیاد رویداد مرتبط با کاربری که آن را ایجاد کرده است، توضیح داده شود. • **آزمون** آزمودن این الزام وابسته به الزام شماره ۱ «تولید داده ممیزی ۱» است. ارزیاب باید رکودهای ممیزی تولیدشده را مطابقت دهد که آیا به نام همان کاربری که آن رویداد را ایجاد کرده، ذخیره‌شده است؟	

۴	**بازبینی داده ممیزی ۱**

محصول باید امکان خواندن/مشاهده [اختصاص: **فهرستی از اطلاعات ممیزی**] از کل رکوردهای ممیزی را برای [اختصاص: **کاربران مجاز**] فراهم نماید.

نکته کاربردی ۲:

- به‌جای کاربران مجاز، با توجه به سازوکار کنترل دسترسی در محصول، کاربران و یا گروه کاربرانی که مجاز به قابلیت خواندن اطلاعات ممیزی هستند را اعلام نماید.
- به‌جای فهرستی از اطلاعات ممیزی، با توجه به سازوکار کنترل دسترسی در محصول، نوع اطلاعات ممیزی که کاربر مجاز قابلیت خواندن آن‌ها را دارد را اعلام نمایید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش از سند هدف امنیتی باید توضیح داده شود که چه مواقعی کاربر قادر به خواندن داده ممیزی است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و تأیید نماید چه زمانی برای کاربر امکان خواندن رکورد ممیزی داده می‌شود و کدام واسط‌هایی این امکان را فراهم می‌کنند.

ارزیاب باید با بررسی سند راهنمای محصول تائید نماید که در این سند در خصوص زمانی که کاربر امکان خواندن رکورد ممیزی دارد و از طریق کدام واسط‌ها این امکان فراهم می‌شود توضیحاتی ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که تنها کاربر با دسترسی مجاز قادر به خواندن رکوردهای ممیزی در فرمت مناسب و قابل‌درک است.

آزمون دوم: ارزیاب باید بررسی کند که با توجه به نوع دسترسی کاربران، اطلاعات و رکوردهای ممیزی مناسب و خاص خود را قادر به خواندن هستند.

۵	**بازبینی داده ممیزی ۲**

محصول باید رکوردهای ممیزی را به شکل خوانا و قابل‌درک برای کاربر نمایش دهد.

اقدامات ارزیابی:

آزمودن این الزام وابسته به الزام شماره ۴ «بازبینی ممیزی امنیت ۱» است.

۶	**بازبینی داده ممیزی ۳**

محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که مجاز به دسترسی هستند (الزام شماره ۴«بازبینی داده ممیزی ۱»)، شود.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی و تأیید نماید چه زمانی برای کاربر امکان خواندن رکورد ممیزی داده می‌شود و کدام واسط‌ها این امکان را فراهم می‌کنند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به خواندن رکوردهای ممیزی است یا خیر.

۷	**بازبینی داده ممیزی ۴**

محصول باید امکان انجام [اختصاص: متدهای انتخاب و مرتب‌سازی] رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را بر اساس [اختصاص: حساب کاربری، تاریخ/زمان، نوع رخداد و [اختصاص: دیگر موارد]] مرتب نماید.

اقدامات ارزیابی:

- **راهنما**

ارزیاب باید سند راهنمای محصول را بررسی کند که نحوه مرتب‌سازی داده‌های ممیزی بیان‌شده است و کدام واسط‌ها این امکان را فراهم می‌کنند.

- **آزمون‌ها**

ارزیاب باید بتواند بر اساس یکی از داده‌های ممیزی، مرتب‌سازی نماید.

۸	**ذخیره‌سازی رویدادهای ممیزی ۱**

محصول باید رکوردهای ممیزی ذخیره‌شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی، مقدار حجم ذخیره‌سازی رکوردهای ممیزی به‌صورت محلی بیان‌شده است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نماید تا در خصوص بیان رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور اطمینان حاصل نماید. برای مثال، اگر رکورد ممیزی تولیدشده باشد، به‌طور هم‌زمان هم در سرور خارجی و هم در محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به‌عنوان بافر مورداستفاده قرار گیرد و با ارسال داده‌ها به‌طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد.

۹	**ذخیره‌سازی رویدادهای ممیزی ۲**

محصول باید قادر به [انتخاب: تشخیص، جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره‌شده، در محل ذخیره‌سازی آن‌ها باشد.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و در خصوص بیان اینکه چه زمانی برای کاربر امکان حذف و یا تغییر رکورد ممیزی داده می‌شود و کدام واسط این امکان را فراهم می‌کند اطمینان حاصل نماید.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به تغییر و یا حذف رکوردهای ممیزی است یا خیر.

آزمون دوم: ارزیاب باید بررسی کند که در صورت تلاش کاربر غیرمجاز برای حذف و یا اعمال تغییرات بر روی رکوردهای ممیزی، در لاگ ذخیره شود.

۱۰	**ذخیره‌سازی رویدادهای ممیزی ۶**

محصول در صورت تجاوز دنباله ممیزی از [اختصاص: یک محدودیت از پیش تعریف‌شده] باید با استفاده از [اختصاص: یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسط‌های محصول کاربران مربوطه را] مطلع نماید.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی مقدار حجم ذخیره‌سازی رکوردهای ممیزی به‌صورت محلی بیان‌شده است. همچنین نوع رویدادی که در صورت پر شدن محل ذخیره‌سازی رخ می‌دهد و چگونگی محافظت از رکوردهای ممیزی در برابر دسترسی‌های غیرمجاز مشخص گردد. در این بخش، عملیاتی که بعد از پر شدن محل ذخیره‌سازی ممیزی صورت می‌گیرد و نوع اطلاعاتی که ممکن است از بین رود باید بیان شود. همچنین نوع تنظیماتی که مدیر سیستم باید بر روی محصول پیکربندی کند تا عملیات موردنظر فعال گردند، باید در این سند تعریف شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید که توضیحاتی در خصوص رویدادهایی که برای پیشگیری از دست رفتن رکوردهای ممیزی در صورت پر شدن محل ذخیره‌سازی در نظر گرفته‌شده، بیان‌شده است.

ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که در خصوص رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور ممیزی توضیحاتی بیان‌شده باشد. برای مثال، اگر رکورد ممیزی تولیدشده باشد، به‌طور هم‌زمان هم در سرور خارجی و هم در محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به‌عنوان بافر مورداستفاده قرار گیرد و با ارسال داده‌ها به‌طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد.

- **آزمون‌ها**

ارزیاب باید مقدار حد آستانه ذخیره‌سازی رکورد ممیزی را به‌گونه‌ای انتخاب نماید که محل ذخیره‌سازی پر شود و بررسی نماید که در این شرایط رویدادهای ادعاشده صورت می‌گیرد.

۱۱	**ذخیره‌سازی رویدادهای ممیزی ۷**

محصول در صورت پر شدن دنباله ممیزی، باید [انتخاب: «رویدادهای ممیزی را نادیده بگیرد»، «از ذخیره رویدادهای قابل ممیزی، به‌جز آن‌هایی که توسط کاربر مجاز و تحت حقوق خاص رخ می‌دهند، جلوگیری نماید»، «روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید»] و [اختصاص: یا دیگر اقدامات برای هشدار از پر شدن فضای ذخیره‌سازی] ارسال نمایند.

۱۲	**انتخاب داده ممیزی ۱**

محصول باید قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی بر اساس مشخصه‌های زیر باشد:

- [انتخاب: هویت موجودیت فعال، نوع رخداد]
- [اختصاص: معیارهای انتخاب دیگر بیان شوند]

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که فهرستی از انواع رویدادها و خصیصه‌های قابل ممیزی وجود دارد که قابل انتخاب می‌باشند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید به ازای هر خصیصه و رویدادی که در لیست آمده است قابل انتخاب بودنشان برای ممیزی را بررسی نماید.

آزمون دوم: ارزیاب باید چندین آیتم از لیست را برای ممیزی انتخاب نموده و بررسی نماید که با اضافه شدن چندین نوع خصیصه و رویداد، عمل به‌درستی اجرا می‌شود.

۶,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۳	**عملیات رمزنگاری ۱ (۱)**
محصول باید [اختصاص: برای وارسی صحت داده‌های ممیزی و داده‌های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری [اختصاص: اندازه‌های کلید رمزنگاری]اجرا شود که مطابق با [اختصاص: فهرستی از استانداردها]باشد. **نکته کاربردی ۳:** روش‌های اطمینان از صحت داده‌ی رکوردها و داده‌ی ممیزی بر عهده نویسنده سند هدف امنیتی است. نویسنده در صورت استفاده از مؤلفه‌های اضافی به‌منظور صحت داده‌ها باید آن‌ها را در سند هدف امنیتی اضافه نماید. ممکن است با توجه به روش بررسی صحت داده نیاز به الزامات ذکرشده در پیوست یک (شماره‌های ۷۸، ۷۹ و ۸۰) باشد لذا لازم است نویسنده سند هدف امنیتی الزامات مرتبط را از پیوست انتخاب و به‌صورت تکمیل‌شده در سند هدف امنیتی ذکر نماید.	
۱۴	**عملیات رمزنگاری ۱(۲)**
محصول باید [اختصاص: تولید داده درهم‌سازی] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری اختصاص: هیچ‌کدام]اجرا شود که مطابق با [اختصاص: فهرستی از استانداردها] باشد. **نکته کاربردی ۴:** از آنجائی که الگوریتم رمزنگاری نیازی به کلید ندارد، محدودیتی برای اختصاص وجود ندارد. در صورت استفاده از کلید رمزنگاری در محصول لازم است. نویسنده سند هدف امنیتی الزامات مرتبط از «پیوست یک» را انتخاب نموده و به‌صورت تکمیل‌شده در سند بیان نماید.	

۶,۳ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۱۵	**مدیریت کلمه عبور**

محصول باید قابلیت‌های مدیریت کلمه عبور را که در زیر ذکرشده‌اند برای کلمه عبورهای مدیریتی فراهم نماید:

۱. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: *"@"، "#"، "$"، "٪"، "^"، "!"، "&"، "*"، "("، ")"* *[اختصاص: کاراکتر دیگر]*] باشد.

۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۱۵ کاراکتر یا بیشتر باشد.

نکته کاربردی ۵:

نویسنده‌ی سند هدف امنیتی، کاراکترهای خاص پشتیبانی شده توسط محصول را انتخاب می‌نماید. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست نماید.

«کلمه عبور مدیریتی» به آن دسته از کلمه عبورهایی اشاره دارد که مدیران از آن‌ها در کنسول محلی یا پروتکل‌هایی که از «کلمه عبور» پشتیبانی می‌نمایند (همچون SSH ,HTTPS)، استفاده می‌کنند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید راهنمای محصول را بررسی نموده تا اطمینان حاصل نماید در این سند توضیحات لازم در خصوص ایجاد کلمه عبورهای قوی و تنظیم طول کلمه عبور برای مدیران بیان‌شده است.

- **آزمون‌ها**

ارزیاب باید کلمه عبورهای ضعیف و قوی ایجاد نموده و عکس‌العمل محصول در خصوص پشتیبانی از هر دو کلمه عبور را بررسی نماید.

ارزیاب باید اطمینان حاصل نماید که تمام کاراکترها، قوانین و حداقل طول کلمه عبور که در سند راهنمای محصول آمده است پشتیبانی می‌گردد.

۱۶	**مدیریت احراز هویت ناموفق ۱**

محصول، باید بتواند با استفاده از [انتخاب: [اختصاص: یک عدد مثبت]، یک عدد مثبت قابل تنظیم توسط مدیر [اختصاص: بازه قابل قبولی از مقادیر]] تلاش ناموفق احراز هویت مرتبط با [اختصاص: فهرستی از رویدادهای احراز هویت] را تشخیص دهد.

نکته کاربردی ۶:

به‌عنوان مثال در سومین اختصاص می‌توان به وارد نمودن کلمه عبور توسط کاربر برای احراز هویت شدن اشاره نمود.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید «خلاصه مشخصات محصول» از سند هدف امنیتی را بررسی نموده تا اطمینان حاصل نماید توضیحاتی در خصوص روش‌های مورد پشتیبانی برای عملیات مدیریتی از راه دور و چگونگی تشخیص تلاش‌های موفق و ناموفق احراز هویت ارائه‌شده است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص دستورات پیکربندی تعداد تلاش‌های موفق و ناموفق احراز هویت، ارائه‌شده است و در صورت استفاده از روش‌های مختلف احراز هویت از راه دور همانند SSH باید در این سند شرح داده شود.

- **آزمون‌ها**

ارزیاب باید بر اساس حد آستانه تلاش موفق و ناموفق احراز هویت در راهنما، محصول را پیکربندی نماید و هنگامی که تعداد تلاش احراز هویت به مقدار حد آستانه رسید با نام کاربری و کلمه عبور معتبر احراز هویت را بررسی کند که در این صورت نباید اجازه ورود دهد.

۱۷	**مدیریت احراز هویت ناموفق ۲**

زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین‌شده رسید، بیشتر از حد تعیین‌شده رسید]، محصول باید [اختصاص: فهرستی از اقدامات مقابله‌ای] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل نماید، توضیحاتی در خصوص نحوه‌ی مدیریت احراز هویت در شرایطی که تعداد تلاش‌های ناموفق احراز هویت به بیش از حد آستانه رسید ارائه‌شده باشد.

۱۸	**تعریف مشخصات کاربر ۱**

محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید:

[انتخاب:

- شناسه کاربر
- متد احراز هویت مورداستفاده
- داده‌های احراز هویت
- نقش کاربر
- وضعیت حساب کاربری (فعال، غیرفعال، بلوکه‌شده و غیره)
- [اختصاص: **هر مشخصه امنیتی دیگر**]

]

نکته کاربردی ۷:

حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باید وجود داشته باشد. این اطلاعات شامل نگهداری نمودن از هر مجوزی است که یک کاربر ممکن است دارا باشد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید بررسی نماید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی مشخصه‌های امنیتی نگهداری شده برای هر کاربر تعریف‌شده باشد. البته ممکن است این لیست با لیست ذکرشده در الزام شماره ۱۸ «تعریف مشخصات کاربر ۱» متفاوت باشد. در این صورت، باید فصل «خلاصه مشخصات محصول» مشخصه‌های امنیتی مهم کاربر را پوشش دهد.

- **سند راهنمای محصول**

ارزیاب باید در راهنمای مدیریتی محصول از سند راهنما توضیحاتی در خصوص ایجاد، مشاهده، تغییر و یا حذف مشخصه‌های امنیتی کاربر (به‌عنوان مثال، تغییر کلمه عبور) مشاهده نماید. • **آزمون‌ها** ارزیاب باید واسط‌های مرتبط با مشخصه‌های امنیتی کاربر را بررسی و آزمون کند.	
۱۹	**شناسایی کاربر ۱**
محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: [انتخاب: • مشاوره راهنمای نحوه ورود به سیستم، • [اختصاص: دیگر اقدامات]] **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب در «خلاصه مشخصات محصول» باید بررسی نماید که اطلاعات ارسالی در احراز هویت راه دور مشخص شده است. • **سند راهنمای محصول** در راهنمای مدیریتی محصول، باید نحوه پیکربندی محصول برای ارتباط با کاربران راه دور توضیح داده شود. • **آزمون‌ها** ارزیاب باید با استفاده از راهنمای محصول پیکربندی مناسبی برای احراز هویت تنظیم نماید؛ بنابراین در اعتبارسنجی/روش احراز هویت، باید نتایج اطلاعات مرتبط با احراز هویت صحیح جهت دسترسی به سیستم فراهم شود. در حالی که در منع دسترسی به سیستم، اطلاعات نادرست فراهم می‌شود.	
۲۰	**شناسایی کاربر ۲**

محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی نماید.	
۲۱	**احراز هویت کاربر ۱**
محصول باید پیش از احراز هویت کاربر، اجازه اقدامات زیر را به کاربر دهد: [انتخاب: • مشاهده راهنمای نحوه ورود به سیستم، • [اختصاص: دیگر اقدامات]	
۲۲	**احراز هویت کاربر ۲**
محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نماید.	
۲۳	**احراز هویت کاربر ۷**
محصول باید به‌منظور احراز هویت کاربر سازوکارهای زیر را فراهم آورد: [انتخاب: • نام کاربری و کلمه عبور • [اختصاص: امضای دیجیتال، یا هر متد احراز هویت جایگزین دیگر برای فراهم آوردن امنیت بهتر]] **نکته کاربردی ۸**: برای احراز هویت کاربر باید بیش از یک سازوکار احراز هویت در محصول به‌کاررفته باشد. به‌عنوان مثال، برای احراز هویت در محصول «نام کاربری و کلمه عبور، گواهی دیجیتال» استفاده می‌گردد.	

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی نماید که سازوکار احراز هویت معرفی‌شده باشد.

- **آزمون‌ها**

برای آزمودن این الزام، ابتدا باید الزام شماره‌ی ۲۱ «احراز هویت کاربر ۱» به‌طور کامل مورد تائید قرارگرفته باشد. سپس ارزیاب باید همه سازوکارهای احراز هویت قابل‌دسترس را پیکربندی نموده و واسط‌های پشتیبان تمام سازوکارهای احراز هویت را بررسی نماید.

۲۴	**احراز هویت کاربر ۸**

محصول باید هر کاربر متقاضی احراز هویت را مطابق [اختصاص: کاربران از راه دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه که در بالا تعریف‌شده استفاده کند، [اختصاص: قوانینی که نحوه سازوکار احراز هویت چندگانه را شرح می‌دهد]] احراز هویت نماید.

اقدامات ارزیابی:

این الزام وابسته به الزام شماره ۲۳ «احراز هویت کاربر ۷» وابسته است.

۲۵	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**

محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:

[انتخاب:

- شناسه کاربر
- نقش‌های کاربر
- جزئیات واسط کلاینت
- پیشینه احراز هویت (زمان آخرین تلاش احراز هویت موفق و ناموفق)
- [اختصاص: لیست دیگر مشخصه‌های کاربری]

]

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید مشخصه‌های امنیتی کاربر که در بخش «خلاصه مشخصات ارزیابی» از سند هدف امنیتی آمده است را با مشخصاتی که در واسط محصول وجود دارد مطابقت دهد تا نسبت به پشتیبانی این الزام اطمینان حاصل نماید.

- **سند راهنمای محصول**

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که نحوه ایجاد موجودیت فعال و امکان تغییر مشخصه‌های امنیتی آن بیان‌شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بتواند بر اساس سند راهنمای محصول، مشخصه‌های امنیتی را برای اجرای عملیات مقداردهی و ویرایش نماید. سپس چگونگی اعمال این تغییرات (موفقیت‌آمیز یا عدم موفقیت) را بررسی نماید. در برخی موارد این آزمون را باید همراه با کنترل دسترسی، محدودیت-های مدیریتی امنیتی و یا در ممیزی صورت گیرد.

آزمون دوم: ارزیاب باید بتواند مشخصه‌های امنیتی را با توجه به راهنمای شرح محصول، با تمامی حداقل شرایط، مقداردهی و یا ویرایش نماید. همچنین ارزیاب با دریافت خطا هنگام بررسی و اعمال مقادیر مختلف در مشخصه‌های امنیتی می‌تواند متوجه شود که تغییرات مشخصه‌های امنیتی به‌درستی اعمال نشده است. در برخی موارد باید این آزمون همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی بررسی شود.

۲۶	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**

محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:

[انتخاب:

- زمانی که یک نشست جدید برقرار می‌شود، اطلاعات موجود از نشست‌های قبلی باید حذف گردد
- اطلاعات پیشینه احراز هویت باید به‌روزرسانی گردد
- [اختصاص: دیگر قوانین برای اتصال اولیه مشخصه‌ها]

]

اقدامات ارزیابی

- **سند راهنمای محصول**

ارزیاب باید در سند راهنمای محصول توضیحاتی در خصوص نحوه‌ی ایجاد موجودیت‌های فعال و اعمال تغییر در مشخصه‌های امنیتی مرتبط با موجودیت‌های فعال مشاهده نماید.

- **آزمون‌ها**

ارزیاب ابتدا نشستی را با محصول آغاز نماید و بعد از محصول خارج شود، ممکن است اطلاعات نشست به‌درستی منقضی نشده باشد لذا لازم است ارزیاب مجدد به سیستم ورود نماید و بررسی نماید که از شناسه نشست قبلی استفاده‌شده است یا خیر.

۲۷	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**

محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید:

[انتخاب: هیچ تغییری در طول نشست فعال مجاز نیست، [اختصاص: دیگر قوانین حاکم بر تغییرات مشخصه‌ها]]

نکته کاربردی ۹:

منظور از تغییرات، به این معناست که هیچ‌یک از مشخصه‌های امنیتی کاربر تعریف‌شده در الزام شماره ۲۵ «انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱» در طول نشست تغییر نکند.

اقدامات ارزیابی

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب ابتدا با یک نام کاربری مشخص نشستی را با محصول آغاز نماید، سپس یکی از مشخصه‌های امنیتی کاربر مانند آدرس IP سیستم را تغییر دهد در این صورت باید نشست غیرفعال و خاتمه یابد.

آزمون دوم: ارزیاب ابتدا نشستی را با محصول با یک نام کاربری مشخص آغاز نماید، سپس اطلاعات نشست را به سیستم دیگر انتقال داده و تلاش نماید با همان اطلاعات نشست اتصال با محصول ادامه داشته باشد. در این حالت به دلیل تغییر آدرس فیزیکی سیستم کاربر باید نشست خاتمه یابد و مجدداً احراز هویت صورت گیرد.

آزمون سوم: ارزیاب ابتدا از طریق نام کاربری و مرورگر مشخص یک نشست با محصول آغاز نماید، سپس با مرورگر دیگری همان اطلاعات نشست را وارد نموده و تلاش نماید اتصال با محصول با همان اطلاعات نشست ادامه داشته باشد. در این صورت باید نشست خاتمه یابد و مجدداً احراز هویت صورت گیرد.

۶,۴ کلاس حفاظت از داده‌های کاربری

شماره الزام	نام الزام
۲۸	**حفاظت از اطلاعات باقیمانده در منابع ۲**
محصول باید تضمین نماید در هنگام [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال استفاده‌شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل‌دسترس می‌گردد. **اقدامات تضمینی:** • **راهنما** در صورت امکان‌پذیری پیکربندی و مدیریت کارکردهای منابع در محصول، انتظار می‌رود که توضیحاتی در خصوص نحوه‌ی پیکربندی مدیریت منابع و استفاده مجدد از آن‌ها در سند راهنمای محصول بخش راهنمای مدیریتی محصول ارائه‌شده باشد. • **آزمون‌ها** ارزیاب باید تمام واسط‌هایی که از منابع استفاده می‌کنند، بررسی نماید؛ همچنین قابل‌دسترس بودن اطلاعات قبلی را در هنگام استفاده مجدد منابع، توسط موجودیت فعال دیگر (یک کاربر دیگر) تجزیه و تحلیل نماید.	
۲۹	**ورود داده‌های کاربری به محصول ۴**
محصول باید هنگام دریافت داده کاربری، [اختصاص: خط‌مشی کنترل دسترسی] را اعمال نماید.	

شماره الزام	نام الزام
اقدامات ارزیابی: • **سند راهنمای محصول** ارزیاب باید در سند راهنمای محصول توضیحاتی در خصوص نحوه‌ی کنترل و همچنین ورود داده کاربری ارائه نماید. • **آزمون‌ها** ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در راهنمای مدیریتی محصول آمده است، کاربری با مجوز ورود داده به داخل سیستم ایجاد نماید و انجام درست عملیات را بررسی و تائید نماید؛ همچنین با کاربری بدون مجوز وارد کردن داده، درستی یا عدم صحت عملیات بررسی گردد.	
۳۰	**ورود داده‌های کاربری به محصول ۵**
محصول باید از مشخصه‌های امنیتی مرتبط با داده‌های کاربری هنگام ورود داده‌ها استفاده نماید. **نکته کاربردی ۱۰:** مشخصه‌های امنیتی داده‌های کاربری می‌تواند شامل نوع داده، اندازه و غیره باشد. **اقدامات ارزیابی** • **آزمون‌ها** این آزمون وابسته به الزام شماره‌ی ۲۹ «ورود داده‌های کاربری به محصول ۴» است. همچنین ارزیاب هنگام ورود داده به سیستم باید اطمینان حاصل نماید که تمامی مشخصه‌های امنیتی کاربر ذکرشده در راهنما همچون نام کاربری و یا امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. این بررسی در عملیاتی مانند «ثبت رکورد ممیزی عملیات ورود» با مشخصه امنیتی کاربر و همچنین «ذخیره داده وارده» با مشخصه امنیتی داده باید بررسی و تائید شود.	
۳۱	**ورود داده‌های کاربری به محصول ۶**
محصول باید اطمینان دهد که پروتکل مورداستفاده برای انتقال، ارتباط و همبستگی بین مشخصه‌های امنیتی و داده کاربری دریافت شده را فراهم می‌نماید.	

شماره الزام	نام الزام
اقدامات ارزیابی • **آزمون‌ها** ارزیاب باید اطمینان حاصل نماید ورود داده به داخل محصول، مطابق پروتکل ادعاشده در سند راهنمای محصول صورت می‌گیرد و در هنگام انتقال شنود و گم شدن داده وجود ندارد.	
۳۲	**ورود داده‌های کاربری به محصول ۷**
محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه فرستنده داده کاربری در نظر گرفته است، است. **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید داده‌ای را مطابق با آنچه در سند راهنما محصول ذکرشده است به محصول ارسال نموده و بررسی نماید که تمام اطلاعات و داده‌ها به‌طور صحیح و کامل انتقال داده‌شده است.	
۳۳	**ورود داده‌های کاربری به محصول ۸**
محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی زیر را اعمال نماید: [اختصاص: قوانین کنترلی اضافی هنگام ورود داده کاربری.] **نکته کاربردی ۱۱:** هدف الزامات مربوط به «ورود داده‌های کاربری به محصول»، ارائه کارکردهایی به‌منظور بررسی و صحت داده ورودی است. به‌عنوان مثال، محصول برای کنترل داده‌های ورودی از سازوکاری همچون امضاء دیجیتال به‌منظور بررسی صحت استفاده نماید یا از مشخصه‌های امنیتی رکوردهای الکترونیکی، همچون خصیصه نوشتنی، خواندنی و غیره محافظت نماید.	

شماره الزام	نام الزام
اقدامات ارزیابی: این الزام وابسته به الزام شماره ۲۹ «ورود داده‌های کاربری به محصول ۴» و الزام شماره ۳۰ «ورود داده‌های کاربری به محصول ۵» است.	
۳۴	**خروج داده‌های کاربری از محصول ۳**
محصول باید هنگام خروج داده کاربری به بیرون[۳] [اختصاص: خط‌مشی کنترل دسترسی] را اعمال نماید. **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در سند راهنمای محصول آمده است، «کاربری دارای مجوز خروج داده از داخل سیستم» ایجاد نموده و صحت انجام عملیات را بررسی نماید؛ سپس چگونگی انجام عملیات را بار دیگر با «کاربری بدون مجوز خروج داده از سیستم» بررسی نماید.	
۳۵	**خروج داده‌های کاربری از محصول ۴**
محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون از محصول)، مشخصه‌های امنیتی مرتبط با داده کاربری را نیز انتقال دهد. **اقدامات ارزیابی:** • **آزمون‌ها** این آزمون وابسته به الزام شماره‌ی ۲۹ «ورود داده‌های کاربری به محصول ۴» است. ارزیاب هنگام خروج داده از سیستم باید اطمینان حاصل کند که مشخصه‌های امنیتی کاربر همانند نام کاربری و یا امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. همچنین باید بررسی گردد برای عملیات خروج با مشخصه امنیتی کاربر، رکورد ممیزی ثبت می‌گردد.	
۳۶	**خروج داده‌های کاربری از محصول ۵**
محصول باید اطمینان دهد که مشخصه‌های امنیتی در هنگام خروج داده از محصول، ارتباط و پیوند شفافی با داده کاربری خارج‌شده دارند.	

[۳] Export user data

شماره الزام	نام الزام
اقدامات ارزیابی: • **آزمون‌ها** این الزام وابسته به الزام شماره‌ی ۲۹ «ورود داده‌های کاربری به محصول ۴» است.	
۳۷	**خروج داده‌های کاربری از محصول ۶**
محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال نماید: [اختصاص: مدیر سیستم باید خروج رکوردها را محدود نماید، به‌طوری‌که کاربران محصول بدون هدف قادر به خروج داده به بیرون از آن (خارج از محصول) نباشند.] **اقدامات ارزیابی:** • **آزمون‌ها** این الزام وابسته به الزام شماره‌ی ۲۹ «ورود داده‌های کاربری به محصول ۴» است.	
۳۸	**صحت داده‌های کاربری ذخیره‌شده ۲**
محصول باید داده کاربری ذخیره‌شده در مکان تحت کنترل خود را برای تشخیص [اختصاص: خطاهای صحت داده] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های [اختصاص: درهم شده[۴] داده‌های کاربری ذخیره‌شده] پایش نماید. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول**	

[۴] Hash

شماره الزام	نام الزام
در این فصل از سند هدف امنیتی باید در مورد پیاده‌سازی تشخیص خطای صحت توضیحاتی بیان‌شده باشد.	
۳۹	**صحت داده‌های کاربری ذخیره‌شده ۳**
هنگام تشخیص خطای صحت داده، محصول باید [اختصاص: اقدام لازم] را صورت دهد. **نکته کاربردی ۱۲:** مشخصه‌های داده کاربری می‌تواند انواع فایل‌ها، اندازه فایل و محتوای فایل باشد. محصول به‌منظور شناسایی خطای صحت داده‌ها باید مشخصه‌های داده‌های کاربری را مانیتور کند تا در صورت تغییر و یا حذف، هشدار دهد. می‌توان برای تشخیص صحت داده‌ها از روش‌هایی همچون HMAC و یا ECC Checksum و دیگر روش‌های درهم‌سازی استفاده نمود.	
۴۰	**خط‌مشی کنترل دسترسی ۱**
محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید: [اختصاص: • موجودیت فعال: [اختصاص: مدیر سیستم، کاربر عادی، [اختصاص: دیگر موجودیت‌های فعال]] • موجودیت غیرفعال: ○ رکوردها، مستندات ○ داده‌های متعلق به کاربر ○ داده احراز هویت ○ داده با این معیارها: [اختصاص: معیارهای داده]	

شماره الزام	نام الزام

- [اختصاص: دیگر موجودیت‌های غیرفعال که شامل خط مش کنترل دسترسی می‌باشند]
- عملیات:
  - ایجاد موجودیت غیرفعال جدید
  - حذف موجودیت غیرفعال
  - تغییر دسترسی‌ها به موجودیت غیرفعال
  - عملیات بر روی فراداده‌های وابسته به موجودیت غیرفعال
  - [اختصاص: دیگر عملیات]

]

اقدامات ارزیابی

- **خلاصه مشخصات محصول**

در این فصل از سند هدف امنیتی، باید سازوکار کنترل دسترسی محصول و مشخصه‌های امنیتی مورداستفاده در خط‌مشی کنترل دسترسی به‌طور خلاصه توضیح داده شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نموده و تائید نماید توضیحاتی در خصوص خط‌مشی کنترل دسترسی و قوانین کنترل دسترسی برای مدیریت مشخصه‌های امنیتی ارائه‌شده است. همچنین ارزیاب باید این سند را در خصوص بیان چگونگی پیکربندی خط‌مشی کنترل دسترسی شامل مقداردهی پیش‌فرض مشخصه‌های امنیتی و انتساب مجوزهای موردنیاز برای عملیات مدیریتی بررسی نماید.

- **آزمون‌ها**

ارزیاب باید برای این الزام موارد زیر را بررسی نماید:

- ✓ تمام الگوریتم‌های کنترل دسترسی ذکرشده در سند هدف امنیتی
- ✓ برای هر الگوریتم کنترل دسترسی تمام شرایط ذکرشده در سند هدف امنیتی باید سنجیده شود (مانند شرایط منتهی شده به "yes" یا "no")

شماره الزام	نام الزام
✓ مجموعه ترکیباتی از تنظیمات مشخصه‌های امنیتی مورداستفاده در الگوریتم‌های کنترل دسترسی همچنین باید برای این الزام کارکردهای مدیریتی مورداستفاده برای مدیریت مشخصه‌های امنیتی (مشخصه‌های امنیتی که در الگوریتم کنترل دسترسی استفاده می‌شوند) آزمون و بررسی شوند.	
۴۱	**عملیات کنترل دسترسی ۱**
محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: [اختصاص: • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند • [اختصاص: دیگر مشخصه‌های موجودیت فعال]] **اقدامات ارزیابی:** الزامات **عملیات** کنترل دسترسی به الزام شماره‌ی ۴۰ «خط‌مشی کنترل دسترسی ۱» وابسته است و همراه با آن الزام بررسی می‌شوند.	
۴۲	**عملیات کنترل دسترسی ۲**
محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [اختصاص: **عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.**]	

شماره الزام	نام الزام
۴۳	**عملیات کنترل دسترسی ۳**

محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد:

[اختصاص:

- کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه‌شده توسط محصول دسترسی دارند.
- کاربران غیرمجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل‌دسترس عموم، دسترسی دارند.
- [اختصاص: دیگر قوانین]

]

۴۴	**عملیات کنترل دسترسی ۴**

محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید:

[اختصاص:

- تجاوز چندین نشست آغازشده با نام کاربری مشابه از مقدار آستانه[۵] از پیش تعریف‌شده،
- [اختصاص: دیگر قوانین]

]

اقدامات ارزیابی:

وابسته به الزام شماره‌ی ۴۳ «عملیات کنترل دسترسی ۳» است.

[۵] Threshold

۶,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۵	**مدیریت کارکرد در محصول ۱**

محصول باید امکان [انتخاب: تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] کارکرد [اختصاص: **تمام کارکردهای مربوط به مدیریت محصول**] را به [اختصاص: **مدیر سیستم،** [اختصاص: دیگر نقش‌ها]] محدود نماید.

نکته کاربردی ۱۳:

مثالی از این اختصاص:

محصول باید امکان «تغییر رفتار» کارکرد جمع‌آوری داده‌های سیستم، آنالیز و عکس‌العمل را تنها به مدیران مجاز سیستم محدود نمایند.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، هریک از کارکرد مدیریتی معرفی‌شده در راهنما (که از طریق واسط قابل‌دسترسی هستند) را بررسی و تائید کند.

- **سند راهنمای محصول**

ارزیاب باید لیست کارکردهای محصول را در این سند بررسی و تائید نماید و همچنین ذکر چگونگی پیکربندی و تنظیمات کارکردها در محصول را بررسی نماید.

- **آزمون‌ها**

ارزیاب باید یک‌بار با مجوز مدیر سیستم سعی در تغییر پیکربندی کارکردهای محصول مطابق با سند راهنمای محصول نماید و بار دیگر با حساب کاربری غیرمجاز تلاش به غیرفعال نمودن و یا تغییر تنظیمات اعمال‌شده در کارکردها نماید.

شماره الزام	نام الزام
۴۶	**مدیریت مشخصه‌های امنیتی ۱**
محصول باید با اعمال [اختصاص: خط‌مشی کنترل دسترسی]، امکان [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، [اختصاص: دیگر عملیات]] مشخصه‌های امنیتی [اختصاص: فهرستی از مشخصه‌های امنیتی تعریف‌شده در الزام انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱] را به [مدیر سیستم، [اختصاص: دیگر نقش‌ها]] محدود نماید. **اقدامات ارزیابی:** • **سند راهنمای محصول** ارزیاب باید سند راهنمای محصول را بررسی نماید و اطمینان حاصل نماید در خصوص شرایطی که یک کاربر اجازه مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال را دارد توضیحاتی ارائه‌شده است. • **آزمون‌ها** ارزیاب باید تمامی واسط‌های مرتبط با مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال و تمام مشخصه‌های امنیتی موجودیت‌های غیرفعال با مقداردهی آن‌ها (البته به‌عنوان بخشی از آزمون الگوریتم کنترل دسترسی در الزام قبل بررسی می‌شوند) را آزمون نماید.	
۴۷	**مدیریت مشخصه‌های امنیتی ۳**
محصول برای مشخصه‌های امنیتی که برای اعمال [اختصاص: خط‌مشی] استفاده می‌شوند، باید مقادیر پیش‌فرض [انتخاب: **محدودشده‌ای]**، در نظر بگیرد. **اقدامات ارزیابی:** به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است.	
۴۸	**مدیریت مشخصه‌های امنیتی ۴**

شماره الزام	نام الزام
محصول برای تعیین مقادیر اولیه پیشنهادی باید به [اختصاص: مدیر سیستم] اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیرفعال، مقادیر پیش‌فرض را لغو و تغییر دهد.	
۴۹	**مدیریت داده‌های محصول ۱-مدیر سیستم**
محصول باید امکان [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [اختصاص: **دیگر کارکردها**]] [اختصاص: **فهرستی از داده‌های محصول]** به [اختصاص: مدیر سیستم، [اختصاص: دیگر نقش‌ها]] محدود نماید. **نکته کاربردی ۱۴:** داده‌های محصول می‌تواند شامل داده‌های ممیزی، کلیدها و داده‌های احراز هویت و از این نوع داده‌ها باشد. مثالی از این الزام: محصول امکان **مدیریت** داده‌های خود را تنها به مدیر امنیتی محدود می‌نماید. «**مدیریت**» در این الزام می‌تواند شامل موارد زیر باشد: ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییر دادن،-حذف نمودن، پاک کردن و اضافه نمودن **اقدامات ارزیابی:** به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است.	
۵۰	**مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده**
محصول باید امکان [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [اختصاص: **دیگر کارکردها**]] [اختصاص: **داده‌های تحت مالکیت کاربر عادی]** را به [اختصاص: کاربر عادی] محدود نماید. **اقدامات ارزیابی:**	

شماره الزام	نام الزام
به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است. همچنین ارزیاب باید حداقل یکی از کارکردهای محصول در این الزام را با کاربری غیرمجاز آزمون نماید.	
۵۱	**کارکردهای مدیریتی محصول ۱**

محصول باید قادر به انجام [اختصاص: کارکردهای مدیریتی که در جدول زیر آمده است] باشد:

مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
ذخیره‌سازی رویدادهای ممیزی ۶	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
ذخیره‌سازی رویدادهای ممیزی ۷	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی ۱	مدیریت مشخصه‌های مورداستفاده برای ایجاد دسترسی و یا منع
حفاظت از اطلاعات باقیمانده در منابع ۲	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزادسازی) که می‌تواند در محصول قابل پیکربندی باشد.
ورود داده‌های کاربری به محصول ۴	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده‌های کاربری ذخیره‌شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق ۱	مدیریت حد آستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.
تعریف مشخصات کاربر ۱	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد.
مدیریت کلمه عبور	مدیریت معیارها برای بررسی کلمه عبورها
احراز هویت کاربر ۱	مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احراز هویت کاربر انجام می‌شوند.
احراز هویت کاربر ۷	مدیریت سازوکارهای احراز هویت

شماره الزام	نام الزام
	مدیریت قوانین مرتبط با احراز هویت
احراز هویت کاربر ۸	مدیریت سازوکارهای احراز هویت مدیریت قوانین مرتبط با احراز هویت
شناسایی کاربر ۱	مدیریت شناسایی کاربر مدیریت لیست عملیاتی که مدیر مجاز می‌تواند قبل از شناسایی کاربر تغییر دهد.
انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و یا تغییر دهد
مدیریت مشخصه‌های امنیتی ۱	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
مدیریت مشخصه‌های امنیتی ۳	مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
مدیریت داده‌های محصول ۱-مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
نقش‌های امنیتی ۱	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
محدودیت بر روی چندین نشست هم‌زمان ۱	مدیریت حداکثر نشست مجاز کاربران به‌طور هم‌زمان توسط مدیر
برقراری نشست ۱	مدیریت شرایط آغاز نشست توسط مدیر مجاز
قفل‌کردن و خاتمه دادن به نشست‌ها ۵	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

تمام کارکردهای امنیتی محصول به‌طور خلاصه باید در این بخش توضیح داده شود.

۵۲	**نقش‌های امنیتی ۱**

شماره الزام	نام الزام
نقش‌های زیر در محصول باید تعریف‌شده باشد: [انتخاب: مدیر سیستم، کاربر عادی، [اختصاص: دیگر **نقش‌های مجاز معرفی‌شده**]] **نکته کاربردی ۱۵:** از جمله نقش‌های مجاز می‌توان به «مدیر مجاز»، «مدیر تحلیلگر مجاز»، «اپراتورها» اشاره نمود، نویسنده سند هدف امنیتی در این الزام می‌تواند از نقش‌های مجاز دیگر نیز استفاده نماید. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب باید در این فصل از سند هدف امنیتی بررسی و تائید نماید توضیحاتی در خصوص نقش مدیریتی و نقش‌هایی با دسترسی پایین ارائه‌شده است. • **سند راهنمای محصول** ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نموده و در خصوص ارائه دستورالعمل‌هایی برای مدیریت محصول هم به‌طور محلی و از راه دور و همچنین پیکربندی‌هایی موردنیاز برای مدیریت راه دور اطمینان حاصل نماید. • **آزمون‌ها** ارزیاب باید اطمینان حاصل نماید که نقش مدیریتی می‌تواند تمامی کارکردهای امنیتی محصول که در سند هدف امنیتی ذکرشده است را مدیریت نماید. ارزیاب باید نقش مدیریتی و یا کاربر با یک نقش محدود را به‌طور محلی و یا از راه دور بر روی محصول آزمون نماید.	

شماره الزام	نام الزام
۵۳	**نقش‌های امنیتی ۲**

محصول، باید قادر به مرتبط نمودن کاربران با نقش‌های مجاز تعریف‌شده باشند.

نکته کاربردی ۱۶:

لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد؛ اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.

اقدامات ارزیابی:

این الزام وابسته به الزام شماره‌ی ۵۲ «نقش‌های امنیتی ۱» است.

۶,۶ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	عنصر امنیتی
۵۴	**حفظ وضعیت امن در زمان شکست ۱**

محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند:

[اختصاص: شکست‌های نرم‌افزاری، شکست‌های کاربری]

شماره الزام	عنصر امنیتی
نکته کاربردی ۱۷: شکست نرم‌افزاری به معنی از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول است که در این صورت محصول باید در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، بررسی نماید توضیحاتی در خصوص پیاده‌سازی شکست امن محصول، انواع مدهای شکست محصول و وضعیت امن هرکدام از شکست‌ها نیز ارائه‌شده باشد. • **آزمون‌ها** ارزیاب باید انواع شکست‌ها را ایجاد و با وضعیت امن مقایسه و بررسی نماید.	
۵۵	**سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۱**
محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [اختصاص: فهرستی از انواع داده‌های امنیتی محصول] را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. **نکته کاربردی ۱۸:** منظور از داده‌های امنیتی محصول، داده‌های احراز هویت، کلید، امضای دیجیتال، داده‌های ممیزی و از این نوع داده‌ها است. **اقدامات ارزیابی:** • **سند راهنمای محصول**	

شماره الزام	عنصر امنیتی
در بخش راهنمای مدیریتی از سند راهنمای محصول باید توضیحاتی در خصوص انواع داده‌های امنیتی محصول و داده‌های دریافتی از دیگر محصولات امن IT ارائه‌شده باشد.	
۵۶	**سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۲**
محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [اختصاص: فهرستی از قوانین تفسیر که در محصول به کار می‌روند] را استفاده نماید. **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید با بررسی داده‌های دریافتی از دیگر محصولات در داخل محصول نسبت به انطباق داده‌های محصول با آنچه ادعای محصول است، اطمینان حاصل نماید.	
۵۷	**انتقال داده امنیتی در داخل محصول ۱**
محصول باید از افشاء یا تغییر داده‌ها در هنگام انتقال بین بخش‌های مجزای خود، محافظت نماید. **نکته کاربردی ۱۹:** منظور از بخش‌های مجزا به این معنی است که بخش‌های محصول بر روی دو سیستم مجزا قرار گرفته باشد، مانند وب سرور بر روی یک سیستم و بانک اطلاعاتی روی سیستم دیگر در یک شبکه عمومی باشد و یا دو بخش مجزای محصول یکی بر روی وب سرور و دیگری بر روی کلاینت باشد. **اقدامات ارزیابی:**	

شماره الزام	عنصر امنیتی
• **خلاصه مشخصات محصول** ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی نماید در خصوص روش یا پروتکل‌های استفاده‌شده برای انتقال داده بین اجزای توزیع‌شده محصول توضیحاتی ارائه‌شده است. • **سند راهنمای محصول** ارزیاب باید با بررسی سند راهنمای محصول، نسبت به ارائه توضیحاتی در خصوص روش یا پروتکل ارتباطی بین اجزای محصول اطمینان حاصل نماید. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید روش ارتباطی ذکرشده در سند راهنمای محصول را آزمون نماید. آزمون دوم: ارزیاب باید اطمینان حاصل نماید که داده‌ها بین اجزای محصول به‌صورت آشکار نمایش داده نشود. آزمون سوم: ارزیاب باید اطمینان حاصل نماید که ویرایش داده‌ها حین انتقال، توسط محصول تشخیص داده شود.	
۵۸	**مهرهای زمانی ۱**
محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب باید اطمینان حاصل نماید در فصل «خلاصه مشخصات محصول» از سند هدف امنیت هریک از کارکردهای امنیتی استفاده‌کننده از زمان لیست شده باشد. • **سند راهنمای محصول**	

شماره الزام	عنصر امنیتی
ارزیاب باید سند راهنمای محصول را بررسی نماید تا در خصوص ارائه‌ی دستورالعمل‌هایی در مورد تنظیمات و پیکربندی زمان اطمینان حاصل نماید. • **آزمون‌ها** ارزیاب باید اقدامات زیر را اجرا کند: آزمون اول: ارزیاب باید مطابق سند راهنمای محصول، زمان را پیکربندی نموده و سپس با توجه به واسط مربوطه از صحت عملکرد آن اطمینان حاصل نماید. آزمون دوم: ارزیاب باید توسط کاربر غیرمجاز و با استفاده از واسط مربوطه، سعی در تغییر پیکربندی زمان نماید. آزمون سوم: اگر محصول از سرور NTP پشتیبانی می‌کند باید کلاینت NTP را بر روی محصول پیکربندی نموده و زمان سرور و کلاینت را بررسی نماید.	
۵۹	**به‌روزرسانی امن ۲**
محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی فراهم نماید که به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را به‌صورت دستی آغاز نماید و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از هیچ مکانیسم به‌روزرسانی دیگری پشتیبانی نکند]. **نکته کاربردی ۲۰:** عبارت «انتخاب» در این الزام بین پشتیبانی از «جستجوی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. جستجوی خودکار به‌روزرسانی‌ها به یک محصول مورد ارزیابی اشاره دارد که جستجو می‌کند تا ببیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به مدیر سیستم اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)؛ اما نصب به‌روزرسانی نیازمند انجام اقداماتی توسط مدیر سیستم خواهد بود؛ اما به‌روزرسانی خودکار به یک محصول مورد ارزیابی اشاره دارد که به‌روزرسانی‌ها را جستجو می‌کند و در صورت وجود آن‌ها را نصب می‌نماید.	

شماره الزام	عنصر امنیتی
۶۰	**به‌روزرسانی امن ۳**
محصول مورد ارزیابی باید در صورت استفاده از به‌روزرسانی به روش خودکار، پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.	

۶,۷ کلاس دسترسی به محصول

شماره الزام	عنصر امنیتی
۶۱	**محدودیت بر روی چندین نشست هم‌زمان ۱**
محصول باید حداکثر تعداد نشست‌های هم‌زمان متعلق به یک کاربر را محدود نماید. **اقدامات ارزیابی:** • **سند راهنمای محصول** ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید توضیحاتی در خصوص نحوه‌ی پیکربندی تعداد نشست هم‌زمان برای یک کاربر در راهنمای محصول ارائه‌شده است. • **آزمون‌ها** ارزیاب باید با توجه به سند راهنمای محصول حداکثر نشست یک کاربر را پیکربندی نماید و سپس با همان کاربر از چند سیستم به‌طور هم‌زمان سعی در ایجاد نشست نماید. در این صورت اگر تعداد نشست بیش از مقدار مشخص شده باشد باید اجازه ایجاد نشست را ندهد.	

شماره الزام	عنصر امنیتی
۶۲	**محدودیت بر روی چندین نشست هم‌زمان ۲**
محصول باید به‌صورت پیش‌فرض، [اختصاص: تعداد نشست هم‌زمان پیش‌فرض] برای هر کاربر در نظر بگیرد. **اقدامات ارزیابی:** وابسته به الزام شماره‌ی ۶۱ «محدودیت بر روی چندین نشست هم‌زمان ۱» است.	
۶۳	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
محصول باید کلیه نشست‌های تعاملی راه دور[۶] را پس از مدت زمان [اختصاص: **بازه زمانی که توسط مدیر تنظیم می‌شود**] غیرفعال بودن، خاتمه دهد. **اقدامات ارزیابی:** • **سند راهنمای محصول** در راهنمای محصول باید در خصوص نحوه‌ی پیکربندی زمان غیرفعال بودن نشست توضیحاتی بیان‌شده باشد. • **آزمون‌ها** ارزیاب باید مطابق سند راهنمای محصول، مقادیر مختلف برای زمان غیرفعال بودن نشست تنظیم و پیکربندی نماید که این مقادیر شامل حداقل و حداکثر زمان غیرفعال بودن طبق سند راهنما باشند. سپس ارزیاب برای هر زمان تنظیم‌شده نشستی از راه دور با محصول ایجاد و درستی زمان غیرفعال بودن نشست را بررسی نماید که باعث خاتمه یافتن نشست می‌شود.	
۶۴	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد. **اقدامات ارزیابی:**	

[۶] Remote

شماره الزام	عنصر امنیتی
• **آزمون‌ها** ارزیاب باید اقدامات زیر را اجرا نماید: آزمون اول: ارزیاب باید نشست محلی با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی نماید که آیا نشست خاتمه یافته است. آزمون دوم: ارزیاب باید نشستی از راه دور با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی نماید که آیا نشست خاتمه یافته است.	
۶۵	**سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به‌طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.	
۶۶	**سوابق دسترسی به محصول ۲**
در صورت برقراری نشست به‌طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] و تعداد تلاش ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد. **اقدامات ارزیابی** • **سند راهنمای محصول** باید در این سند در خصوص نحوه‌ی پیکربندی نمایش تعداد و آخرین تلاش ناموفق توضیحاتی ارائه‌شده باشد. • **آزمون‌ها** ارزیاب چندین بار با استفاده از یک نام کاربری با شرایطی غیرمجاز (مانند کلمه عبور نادرست) تلاش به برقراری نشست با محصول نماید و سپس یک نشست موفقیت‌آمیزی را برقرار نماید و بررسی نماید که تعداد تلاش‌های ناموفق کاربر و زمان آخرین تلاش برای برقراری نشست در محصول ثبت‌شده باشد.	

شماره الزام	عنصر امنیتی
۶۷	**سوابق دسترسی به محصول ۳**
محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک نماید. **اقدامات ارزیابی** • **سند راهنمای محصول** در صورت وجود امکان پیکربندی اطلاعات سوابق دسترسی، باید در بخش راهنمای مدیریتی از سند راهنمای محصول توضیحاتی ارائه‌شده باشد.	
۶۸	**برقراری نشست ۱**
محصول باید قادر به ممانعت از ایجاد نشست بر اساس [انتخاب: مکان، شماره پورت، روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد. **اقدامات تضمینی:** • **خلاصه مشخصات محصول** ارزیاب باید با بررسی فصل «خلاصه مشخصات محصول» از سند هدف امنیتی نسبت به تعریف تمام مشخصه‌های کلاینتی که باید نشست آن منع شود، اطمینان حاصل نماید. • **راهنما** ارزیاب باید در سند راهنمای محصول، بررسی نماید توضیحاتی در خصوص پیکربندی هر مشخصه‌ای که در «خلاصه مشخصات محصول» آمده است (مشخصه‌هایی مانند آدرس IP ، زمان/تاریخ، آدرس فیزیکی و ...) ارائه‌شده است. • **آزمون‌ها** ارزیاب باید برای هر یک از مشخصه‌ها، آزمون زیر را انجام دهد: آزمون اول: ارزیاب باید با یک کاربر یک نشست موفقیت‌آمیزی را ایجاد نماید، سپس مطابق راهنما، مشخصه‌های کاربر را به‌گونه‌ای پیکربندی نماید که از دسترسی آن کاربر به محصول ممانعت شود. ارزیاب باید تلاش در برقراری نشستی نماید که مشخصه‌ای از آن (مانند آدرس IP و یا مکان کاربر) برای دسترسی منع شده باشد و سپس عدم موفقیت کاربر در تلاش برای دسترسی را مشاهده نماید.	

۶,۸ کلاس تخصیص منابع

شماره الزام	عنصر امنیتی
۶۹	تحمل خطا ۱
محصول باید از عملکرد [اختصاص: تمام کارکردهای اصلی] هنگام رویداد شکست‌های زیر اطمینان حاصل نماید: [اختصاص: شکست نرم‌افزاری، [اختصاص: انواع دیگر شکست‌ها]] **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید شکستی را ایجاد و سپس بررسی نماید که کارکردهای اصلی (مانند ممیزی) به‌درستی کار می‌کنند یا خیر.	

۶,۹ کلاس کانال‌ها/مسیرهای مورد اعتماد

برای این کلاس، تعدادی الزام مبتنی بر انتخاب در «پیوست دو» ارائه‌شده است.

شماره الزام	نام الزام
۷۰	مسیر امن ۱

شماره الزام	نام الزام
محصول باید با استفاده از پروتکل [انتخاب: TLS, HTTPS] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه دور ایجاد شود که به‌طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد. **نکته کاربردی ۲۱:** کاربر عمومی مجوز ورود به محصول را ندارد. نویسنده سند هدف امنیتی در صورت استفاده از TLS باید الزامات آن را از «پیوست دو» به سند هدف امنیتی اضافه نماید.	
۷۱	**مسیر امن ۲**
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۷۲	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی نماید. **نکته کاربردی ۲۲:** این الزام اطمینان حاصل می‌نماید که مدیران سیستم معتبر، تمام ارتباطات از راه دور را با محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل‌شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت انتخاب، رمزگذاری می‌شوند.	

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف‌شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی‌شده در بخش ۴ در نظر گرفته‌شده‌اند. الزامات کارکردی در بخش ۶ بیان رسمی و استانداردی از «اهداف امنیتی» است. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا بر اساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل بر روی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به‌صورت زیر است:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول را در اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌نماید؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح‌شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۷,۱ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نیست، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسط‌های کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسط‌ها نیست. فعالیت‌های این خانواده باید بر روی شناخت واسط‌های معرفی‌شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه‌شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند،

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح‌شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نیست.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورداستفاده برای هر واسط اجراکننده کارکرد امنیتی[۷] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۸] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱

[۷]-SFR-enforcing TSFI
[۸]-SFR-supporting TSFI

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مؤلفه: (ADV_FSP.1.3C) **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به‌واسطه کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده است.

۷,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به‌عنوان یک محصول و به‌عنوان بخشی از یک محیط عملیاتی بزرگ‌تر

دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت‌شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۷,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط محصول به‌صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به‌صورت مناسبی تعیین نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده‌شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: سند راهنمای کاربردی باید واضح و قابل‌فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
	ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به‌صورت امن برای عمل نمودن آماده شود.

۷,۳ کلاس آزمون

آزمودن محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمودن بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمودن بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته‌شده است.

۷,۳,۱ آزمون مستقل

«آزمون مستقل» برای تائید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه‌شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آزمون مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)**

مؤلفه‌های اقدامات ارزیاب	
	شرح مؤلفه: ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به‌صورت مشخص شده عمل می‌نمایند.

۷,۴ کلاس آسیب‌پذیری

۷,۴,۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۷,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه‌شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل‌مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۷,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به‌صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه‌شده، است (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به‌تنهایی، برچسب‌گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به‌آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود محصول و مدارک موردنیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به‌صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۸ پیوست یک:: الزامات کلاس پشتیبانی از رمزنگاری مبتنی بر انتخاب

شماره الزام	نام الزام
۷۳	**مدیریت کلید رمزنگاری ۱**

محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر تولید کنند.

[انتخاب:

- *استفاده از طرح RSA با اندازه کلید 2048 بیت یا بیشتر که از این اسناد پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.3*
- *استفاده از طرح ECC "NIST curves" [انتخاب: P-256، P-384، P-521] که از اسناد زیر پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.4*

نکته کاربردی ۲۳:

نویسنده سند هدف امنیتی تمام طرح‌های تولید کلید که برای استقرار و احراز هویت کاربران استفاده می‌شود را انتخاب می‌کند. وقتی کلید تولیدشده برای احراز هویت کاربران استفاده می‌شود، انتظار می‌رود کلید عمومی با یک گواهی X.509v3 مرتبط گردد.

در صورتی که محصول به‌عنوان یک گیرنده در طرح استقرار کلید RSA عمل نماید، نیاز به پیاده‌سازی تولید کلید RSA نیست.

۷۴	**مدیریت کلید رمزنگاری ۴**

شماره الزام	نام الزام
محصول باید بر اساس متد تخریب کلید رمزنگاری [اختصاص: **متد تخریب کلید رمزنگاری**] که بر اساس استاندارد [اختصاص: **فهرستی از استانداردها**] باشد، کلیدهای رمزنگاری را از بین ببرد. **اقدامات تضمینی:** • **خلاصه مشخصات محصول** ارزیاب باید این بخش را بررسی کند که در مورد همه کلیدهای محرمانه توضیحاتی بیان‌شده باشد. همچنین در مورد روش رویه تخریب کلید در حافظه (به‌عنوان مثال، بازنویسی با صفر و غیره) توضیحاتی را بیان نماید.	
۷۵	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۳)**
محصول باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری متقارن AES- XTS مطابق مستند NIST SP 800- 38E, AES-CBC مطابق سند NIST SP 800- 38A AES-CCMP مطابق سند FIPS PUB 197، NIST SP 800- 38C و IEEE 802.11 2012 و [انتخاب: AES Key Wrap (KW مطابق سند NIST SP 800-38F, AES Key Wrap with Paddi ng (KWP مطابق سند NIST SP 800-38F، AES-GCM مطابق سند NIST SP 800-38D, AES-CCM مطابق سند NIST SP 800-38C,	

شماره الزام	نام الزام
	AES-CCMP-256مطابق سند NIST SP800-38C و IEEE 802.11 ac-2013, AES-GCMP-256مطابق سند NIST SP800-38D و IEEE 802.11 ac-2013 و هیچ‌کدام] با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.
۷۶	**عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید خدمات امضای دیجیتال (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوی RSA: اندازه کلیدهای [انتخاب: ۲۰۴۸ بیتی یا بزرگ‌تر] و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS» بخش ۴ • در مورد الگوی دیجیتال بیضوی ECDSA: اندازه کلیدهای [انتخاب: ۲۵۶ بیتی یا بزرگ‌تر] با استفاده از منحنی‌های NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵] **نکته کاربردی ۲۴:** نویسنده هدف امنیتی باید الگوریتم مورداستفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین نماید.	

۹ پیوست دو: الزامات پروتکل TLS مبتنی بر انتخاب

با استفاده از پروتکل‌های زیر می‌توان تهدیدات مرتبط با به خطر افتادن کانال ارتباطی بین مدیران و دیگر بخش‌های محصول یا موجودیت‌های IT خارجی را کاهش داد. برای حفاظت از اتصال سرور ممیزی و مدیران راه دور باید از یکی از پروتکل‌های ارتباطی امن (TLS ، TLS/HTTPS) استفاده نمود.

شماره الزام	نام الزام
۷۷	**الزامات پروتکل TLS Server/ احراز هویت ۱**

محصول باید [انتخاب: TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:

- مجموعه‌های رمز اجباری:
- [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268]
- [انتخاب: مجموعه‌های رمز اختیاری:
  - LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246

○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289 • هیچ مجموعه رمز دیگری]]. **نکته کاربردی ۲۵:** مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدود شده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
الزامات پروتکل TLS Server/ احراز هویت ۲	**۷۸**
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0و [انتخاب: TLS1.1، هیچ‌کدام] دارند، رد نماید. **نکته کاربردی ۲۶:** تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکل TLS Server/ احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.	
الزامات پروتکل TLS Server/ احراز هویت ۳	**۷۹**

محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری] ،[انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید.

نکته کاربردی ۲۷:

اگر در بخش «الزامات پروتکل TLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند ST باید شامل Diffie-Hellman یا منحنی‌هایNIST لیست شده در این الزام باشد.

۱۰ پیوست سه: الزامات کلاس ممیزی مبتنی بر انتخاب

جدول زیر مربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب است. همان‌طور که در بخش‌های قبلی هم مطرح‌شده بود، در صورت نیاز به این جدول برای ثبت اطلاعات ممیزی باید مراجعه کرد.

مؤلفه	رویداد قابل ممیزی	جزئیات
انتخاب داده ممیزی ۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
ذخیره‌سازی رویدادهای ممیزی ۶	عملیات انجام‌شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	

ذخیره‌سازی رویدادهای ممیزی ۷	عملیات انجام‌شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
عملیات رمزنگاری ۱(۱)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات رمزنگاری ۱ (۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی ۱	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	شناسایی داده‌های موجودیت غیرفعال
ورود داده‌های کاربری به محصول ۴	ورود داده کاربری موفقیت‌آمیز، شامل هرگونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هرگونه مشخصه‌های امنیتی (پایه)	
خروج داده‌های کاربری از محصول ۳	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	
مدیریت کارکرد در محصول ۱	تمامی تغییرات در رفتارهای کارکردی محصول	
کارکردهای مدیریتی محصول ۱	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
نقش‌های امنیتی	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش است (حداقل)	
سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از سازوکار سازگاری داده‌های محصول (حداقل) ثبت استفاده از سازوکار سازگاری داده‌های محصول (پایه)	

محدودیت بر روی چندین نشست هم‌زمان	ثبت رد یک نشست مبتنی بر محدودیت نشست‌های هم‌زمان (حداقل)	
قفل‌کردن و خاتمه دادن به نشست‌ها ۵	ثبت خاتمه دادن به یک نشست بیکار توسط سازوکار قفل نشست (حداقل)	
قفل‌کردن و خاتمه دادن به نشست‌ها ۶	ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	