به نام خدا

سند هدف امنیتی
سامانه اداری فرضی
نسخه ۱,۱

شرکت X

فروردین ۹۵
نسخه ۱,۰

فهرست

با تشکر از همکاری شرکت

علوم راهبردی ایده

۱ معرفی سند هدف امنیتی

۱,۱ مرجع سند هدف امنیتی و مرجع هدف ارزیابی

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه اداری فرضی
نسخه	۱,۰
تاریخ	فروردین ۹۵
نویسندگان	گروه توسعه شرکت X

نام تولید کننده (شرکت)	شرکت X
نام هدف ارزیابی	سیستم
نوع هدف ارزیابی	برنامه کاربردی تحت وب
نسخه	۱,۱

نرم‌افزار/سخت‌افزار/میان‌افزار غیر هدف ارزیابی

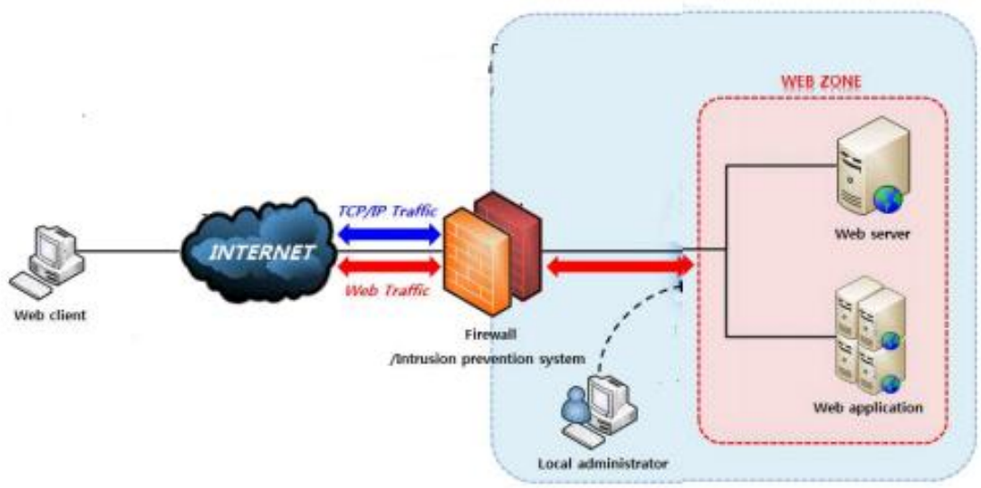
در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای اجرای و کارکرد هدف ارزیابی لیست شده‌اند:

کامپوننت‌ها	حداقل الزامات
پردازنده	Intel Dual Xeon Processor X5690(3.46 GHz, 6-core, 12Mb Cache, 130W, DDR3 –1333)
فضای آزاد دیسک	۳۰۰ GB
حافظه	8 GB or Higher
سیستم عامل	Windows 2008 Enterprise R2 or higher (2012 recommended)
DBMS	SQL Server 2008 R2 Enterprise or higher (2014 recommended)
سایر نرم افزارها	MS SQL SSRS - .Net Framework 4.0

۱,۲ شرح محصول

حوزه فیزیکی

(حوزه فیزیکی مشخص شده فرضی می‌باشد.)



حوزه منطقی

کارکردها	توصیف
احراز هویت با استفاده از Active Deirectory	ارتباط نرم افزار با سرور Active Directory و شناسایی هویت فرد
رویداد نگاری	مشاهده تمامی فعالیت های انجام شده توسط کاربران
Login به نرم افزار با استفاده از Web service	ارتباط نرم افزار با Web Service و شناسایی هویت فرد
کنترل دسترسی	هدف ارزیابی دارای امکان دسترسی محدود میباشد، به طوریکه تنها موجودیت های مجاز خاص دارای دسترسی به داده و کارکردهای هدف ارزیابی هستند.برای کاربران مجاز کنترل دسترسی معمولا با استفاده از داده احراز هویت انجام میگیرد.

۲ ادعای انطباق

۲,۱ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO/IEC 15408, version 3.1, revision 4, september 2012
نام پروفایل حفاظتی	پروفایل حفاظتی سامانه اداری کلاینت سرور نسخه ۱,۰
سطح تضمین امنیتی	EAL 1

۳ مسائل امنیتی

۳,۱ 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 ایجاد شده 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 حفاظت شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نمی‌باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. و 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 می‌باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از رکوردهای ممیزی جلوگیری کند (به عنوان 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 وارد کننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می‌تواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص می‌باشد که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDoS می‌باشد 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 رابه 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.

۳,۲ خط‌مشی امنیتی

خط مشی ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می‌گیرند.
ارتباطات امن مبتنی بر TLS	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مولفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده 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 به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳,۳ فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
محیط امن	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده 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 ایجاد شده یا وارد شده توسط محصول، واحد ذخیره‌سازی و دیگر مولفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند، و بنابر 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 مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال 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 اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۴ اهداف امنیتی

۴,۱ 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 به موقع از رخداد امنیتی بحرانی آگاه نماید.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصول باید برای کاربران به صورت 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 احرازهویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت 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 تعریف شده 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.
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد 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.

هدف امنیتی	توضیحات
مدیریت خطا	محصول باید صورت امن و کارامد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت 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 رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صور رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده‌های باقیمانده	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می‌گردد.

۴,۲ 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 مولفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده‌ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می‌باشد. 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 استفاده شده به منظور تست باید پاک یا غیر قابل دسترس گردند.

اهداف امنیتی محیطی	توضیحات
پشتیبان-گیری 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 تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

۵ الزامات کارکرد امنیتی

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

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	**ذخیره سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۹	**ذخیره سازی رویدادهای ممیزی ۲**	FAU_STG.1.2
۱۰	**ذخیره سازی رویدادهای ممیزی ۷**	FAU_STG.4.1
۱۱	**انتخاب داده ممیزی ۱**	FAU_SEL.1.1
۱۲	**مدیریت کلید رمزنگاری ۱**	FCS_CKM.1.1
۱۳	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی 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	**احراز هویت کاربر ۱**	FIA_UAU.1.1
۲۱	**احراز هویت کاربر 2**	FIA_UAU.1.2
۲۲	**احرازهویت کاربر ۷**	FIA_UAU.5.1
۲۳	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱**	FIA_USB.1.1
۲۴	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲**	FIA_USB.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۵	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۲۶	ورود داده های کاربری به محصول ۴	FDP_ITC.2.1
۲۷	ورود داده های کاربری به محصول ۵	FDP_ITC.2.2
۲۸	ورود داده های کاربری به محصول ۶	FDP_ITC.2.3
۲۹	خروج داده های کاربری از محصول ۳	FDP_ETC.2.1
۳۰	صحت داده های کاربری ذخیره شده ۲	FDP_SDI.2.1
۳۱	صحت داده های کاربری ذخیره شده ۳	FDP_SDI.2.2
۳۲	خط مشی کنترل دسترسی ۱	FDP_ACC.1.1
۳۳	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۳۴	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۳۵	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۳۶	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۳۷	مدیریت مشخصه‌های امنیتی 1	FMT_MSA.1.1
۳۸	مدیریت مشخصه های امنیتی ۳	FMT_MSA.3.1
۳۹	مدیریت مشخصه های امنیتی ۴	FMT_MSA.3.2
۴۰	مدیریت داده های محصول ۱-مدیر سیستم	FMT_MTD.1.1(1)
۴۱	مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده	FMT_MTD.1.1(2)
۴۲	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۴۳	نقش‌های امنیتی ۱	FMT_SMR.1.1
۴۴	نقش‌های امنیتی ۲	FMT_SMR.1.2
۴۵	لغو مشخصه های امنیتی ۱	FMT_REV.1.1
۴۶	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۴۷	سازگاری داده های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۴۸	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۴۹	مهرهای زمانی ۱	FPT_STM.1.1
۵۰	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۱	محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
۵۲	قفل کردن و خاتمه دادن به نشست ها ۵	FTA_SSL.3.1
۵۳	قفل کردن و خاتمه دادن به نشست ها ۶	FTA_SSL.4.1
۵۴	سوابق دسترسی به محصول ۱	FTA_TAH.1.1
۵۵	کانال امن ۱	FTP_ITC.1.1
۵۶	کانال امن ۲	FTP_ITC.1.2
۵۷	کانال امن ۳	FTP_ITC.1.3
۵۸	مسیر امن ۱	FTP_TRP.1.1
۵۹	مسیر امن ۲	FTP_TRP.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۰	**مسیر امن ۳**	FTP_TRP.1.3
۶۱	**به روز رسانی امن ۲**	FPT_TUD_EXT.1.2
۶۲	**به روز رسانی امن ۳**	FPT_TUD_EXT.1.3
الزامات پیوست یک		
۶۳	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۶۴	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۶۵	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۶۶	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۶۷	الزامات پروتکل IPSEC (۲)	FCS _IPSEC_EXT.1.2
۶۸	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۶۹	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۷۰	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۷۱	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۷۲	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۷۳	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۷۴	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۷۵	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۷۶	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۷۷	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۷۸	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۷۹	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۸۰	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۸۱	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۸۲	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۸۳	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۸۴	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۸۵	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۸۶	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۸۷	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۸۸	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۸۹	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۹۰	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۹۱	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
۹۲	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۹۳	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۹۴	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۹۵	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۹۶	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8

شماره الزام	نام الزام	تطابق الزام با استاندارد
۹۷	الزامات پروتکلTLS Client/ احراز هویت ۱	FCS_TLSC_EXT.1.1
۹۸	الزامات پروتکلTLS Client/ احراز هویت ۲	FCS_TLSC_EXT.1.2
۹۹	الزامات پروتکلTLS Client/ احراز هویت ۳	FCS_TLSC_EXT.1.3
۱۰۰	الزامات پروتکلTLS Client/ احراز هویت ۴	FCS_TLSC_EXT.1.4
۱۰۱	الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۱	FCS_TLSC_EXT.2.1
۱۰۲	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۲	FCS_TLSC_EXT.2.2
۱۰۳	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۳	FCS_TLSC_EXT.2.3
۱۰۴	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۴	FCS_TLSC_EXT.2.4
۱۰۵	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۵	FCS_TLSC_EXT.2.5
۱۰۶	الزامات پروتکلTLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
۱۰۷	الزامات پروتکلTLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
۱۰۸	الزامات پروتکلTLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
۱۰۹	الزامات پروتکلTLS Server/ احرازهویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۱۰	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۱۱	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۱۲	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۴	FCS_TLSS_EXT.2.4
۱۱۳	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۵	FCS_TLSS_EXT.2.5
۱۱۴	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۶	FCS_TLSS_EXT.2.6
۱۱۵	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۱۱۶	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۱۱۷	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۱۱۸	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
۱۱۹	الزامات پروتکل X509 (۵)	FIA_X509_EXT.3.1
۱۲۰	الزامات پروتکل X509 (۶)	FIA_X509_EXT.3.2

۵,۱ کلاس ممیزی امنیت

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

محصول می تواند براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:

- ورود و خروج کاربر به/ از سیستم
- رویدادهای قابل ممیزی (این رویدادها در جدول زیر آمده است)،

مولفه	رویداد قابل ممیزی	جزئیات
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی	
بازبینی داده ممیزی ۳	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی	

ذخیره سازی رویدادهای ممیزی ۷	عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی	به دلیل ذخیره سازی داده های ممیزی در پایگاه داده بروز چنین مشکلی امکان پذیر نمی باشد. یعنی اگر احتمال بروز چنین آسیب پذیری وجود داشت یعنی تنظیمات پایگاه داده درست ست نشده که در این صورت به طور کلی نرم افزار اجرا نخواهد شد.
عملیات کنترل دسترسی ۱	تمامی درخواست‌های ناموفق برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	
مدیریت کلمه عبور	تلاش موفق و ناموفق ورود کاربر	تمامی درخواست های ورود اعم از موفق یا نا موفق در سیستم ثبت می گردد.
مدیریت مشخصه‌های امنیتی1	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد.
مدیریت داده های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی	
مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد.
تغییرات روی موجودیت های غیر فعال	افزودن، ویرایش، حذف موجودیت های غیر فعال	
تغییرات روی موجودیت های فعال	افزودن، ویرایش، حذف موجودیت های فعال	
تعلیق ورود موجودیت فعال	جلوگیری از ورود کاربر پس از ۴ بار تلاش ورود ناموفق	

۲	**تولید داده ممیزی ۲**

محصول می تواند برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

- تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد
- نوع کاربری، IP کاربر، محل خدمت کاربر

۳	**تولید داده ممیزی ۳**

برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول می تواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید.

۴	**بازبینی داده ممیزی ۱**

محصول می تواند امکان خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش،حذف و ایجاد آیتم جدید،صدور مجوز و گواهینامه، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم فراهم نماید.

۵	**بازبینی داده ممیزی ۲**

محصول می تواند رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر نمایش دهد.

۶	**بازبینی داده ممیزی ۳**

محصول می تواند از دسترسی کلیه کاربران به جز کاربرانی که به آنها مجوز دسترسی خواندن داده شده باشد (الزام شماره ۴) جهت خواندن رکوردهای ممیزی ممانعت نماید.

۷	بازبینی داده ممیزی ۴
محصول می تواند امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس مرکز برگزار کننده، کاربر، نوع کاربری، تاریخ، موضوع و نوع رخداد(عملیات) مرتب نماید.	
۸	ذخیره سازی رویدادهای ممیزی ۱
محصول می تواند رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت نماید. از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد. کاربر تنها در صورتی امکان حذف داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات حذف را انجام دهد که در آن حالت عملیات پیش گفته در پایگاه داده به طور خودکار ممیزی می شود.	
۹	ذخیره سازی رویدادهای ممیزی ۲
محصول قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در محل ذخیره سازی آنها می باشد.	
۱۰	ذخیره سازی رویدادهای ممیزی ۷
محصول در صورت پر شدن محل ذخیره‌سازی رکورد ممیزی «از ذخیره رویدادهای قابل ممیزی، بجز آنهایی که توسط مدیر سیستم تعیین می گردد، جلوگیری نماید و هشدار لازم را با استفاده از **پیام کوتاه**، مدیر سیستم را مطلع نماید ».	
۱۱	انتخاب داده ممیزی ۱
محصول می تواند قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه‌های زیر باشد: • هویت موجودیت فعال، نوع رخداد (عملیات) • گروه کاربری • محدوده زمانی • موضوع، فرم، IP	

۵,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۲	تولید کلید رمزنگاری ۱
محصول می تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر تولید کنند. 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.	
۱۳	عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۱)
محصول می تواند **رمزنگاری و رمزگشایی** را مطابق با الگوریتم رمزنگاری متقارن AES Key Wrap with Paddi ng (KWP مطابق سند NIST SP 800-38F ، با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.	

شماره الزام	نام الزام
۱۴	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی می تواند خدمات امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم رمزنگاری زیر ارائه کند: الگوی RSA: اندازه کلیدهای ۲۰۴۸ بیتی و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)» بخش ۴	

۵,۳ کلاس شناسایی و احرازهویت

شماره الزام	نام الزام
۱۵	**مدیریت کلمه عبور**
محصول می تواند قابلیت‌های مدیریت رمزعبور را که در زیر ذکر شده‌اند برای رمزهای عبور مدیریتی فراهم نماید: ۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص"!"، "@"، "#"، "$"، "٪"، "*"، "(" ، ")"، "_"، "+"، "^"، "&"، "}"، "{"، ":"، ";"، "?"، "." باشند. ۲. حداقل طول رمزعبور باید توسط مدیر امنیت، قابل تنظیم باشد.	
۱۶	**مدیریت احراز هویت ناموفق ۱**
محصول می تواند با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نماید.	
۱۷	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید و یا از آن بیشتر شد، محصول می تواند عملیات "جلوگیری از ورود کاربر به مدت تعیین شده توسط مدیر" اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.	
۱۸	**تعریف مشخصات کاربر ۱**
محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: • شناسه کاربر داده های احراز هویت • نقش کاربر • وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره) • IP کاربر • رمز عبور کاربر	
۱۹	**شناسایی کاربر ۱**
محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: • **مشاوره راهنمای نحوه ورود به سیستم،**	
۲۰	**احراز هویت کاربر ۱**
محصول می‌واند پیش از احراز هویت کاربر، اجازه اقدامات زیر را به کاربر دهد: • بازیابی رمز عبور	
۲۱	**احراز هویت کاربر ۲**

محصول می تواند هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نماید.	
۲۲	**احراز هویت کاربر ۷**
محصول باید اقدامات زیر را برای احرازهویت کاربر فراهم آورد: • نام کاربری و کلمه عبور • احراز هویت از طریق Active Directory	
۲۳	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**
محصول می تواند مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: • شناسه کاربر • نقش‌های کاربر • جزئیات واسط کلاینت (مرورگر ، IP) • پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق) تا ۳۰ دقیقه گذشته • پیشینه دسترسی به سند/رکورد اخیر(ممیزی)	
۲۴	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲**
محصول می تواند قوانین زیر را بر روی اتصال اولیه کاربر فعال اعمال نماید: • زمانی‌که یک نشست جدید برقرار می‌شود، اطلاعات موجود از نشست‌های قبلی باید حذف گردد. • اطلاعات پیشینه احراز هویت باید بروزرسانی گردد. • ثبت رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید	
۲۵	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳**
محصول قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: **هیچ تغییری در طول نشست فعال مجاز نمی‌باشد.**	

۵,۴ کلاس حفاظت از داده‌های کاربری

شماره الزام	نام الزام
۲۶	**ورود داده های کاربری به محصول ۴**
محصول هنگام دریافت داده کاربری، **خط‌مشی کنترل دسترسی، فرمت‌های مجاز داده‌ها (.jpg,docx)** را اعمال می‌نماید.	
۲۷	**ورود داده های کاربری به محصول ۵**
محصول می تواند از مشخصه‌های امنیتی مرتبط با داده‌های کاربری را هنگام ورود داده‌ها استفاده نماید.	
۲۸	**ورود داده های کاربری به محصول ۶**

شماره الزام	نام الزام
محصول می تواند اطمینان دهد که پروتکل مورد استفاده برای انتقال، ارتباط و همبستگی بین مشخصه‌های امنیتی و داده کاربری دریافت شده را فراهم می‌نماید.	
۲۹	**خروج داده های کاربری از محصول ۳**
محصول می تواند هنگام خروج داده کاربری به بیرون داده ها را در سه فرمت (pdf,word, Excel) نمایش داده و از خروج داده های حساس مانند نام کاربری و کلمه عبور و ایمیل کاربر جلوگیری کند.	
۳۰	**صحت داده های کاربری ذخیره شده ۲**
محصول می تواند داده کاربری حساس ذخیره شده در مکان تحت کنترل خود را براساس مشخصه‌های رمزنگاری امن نگهداری کرده و به منظور شناسایی خطای صحت داده رکورد و داده ممیزی، پایش نماید.	
۳۱	**صحت داده های کاربری ذخیره شده ۳**
هنگام تشخیص خطای صحت داده، محصول می تواند ثبت ممیزی را صورت دهد.	
۳۲	**خط مشی کنترل دسترسی ۱**

محصول می تواند دسترسی بر اساس نوع کاربری که هنگام ورود کاربر شناسایی می شود را بر روی موارد زیر اعمال نماید:

- **موجودیت های فعال به تفکیک ماژول های سیستم**

نرم افزار مدیریت اموزش

- مدیر سیستم
- مدیر استانی

نرم افزار سامانه فراگیر

- فراگیر
- مدرس

نرم افزار یادگیری الکترونیکی

- مدیر سیستم
- فراگیر
- مدرس

- **موجودیت غیرفعال:**
  - رکوردها، مستندات
  - داده‌های متعلق به کاربر
  - داده احرازهویت
  - داده با این معیارها: عکس کاربر با فرمت های BMP, PNG, JPG,GIF
  - کلاس های آموزشی
  - دوره های آموزشی
- **عملیات:**
  - ایجاد موجودیت غیرفعال جدید
  - انتقال موجودیت غیرفعال
  - ویرایش و حذف موجودیت غیر فعال
  - ایجاد موجودیت فعال جدید
  - انتقال موجودیت فعال

شماره الزام	نام الزام
○ ویرایش و حذف موجودیت فعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فراداده‌های وابسته به موجودیت غیرفعال	
۳۳	**عملیات کنترل دسترسی ۱**
محصول می تواند سطح دسترسی را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند	
۳۴	**عملیات کنترل دسترسی ۲**
محصول می تواند قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نمایند: 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 تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.	
۳۵	**عملیات کنترل دسترسی ۳**
محصول می تواند براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه شده توسط محصول دسترسی دارند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.	

۵,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۳۶	**مدیریت کارکرد در محصول ۱**
محصول می تواند توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر سیستم محدود نماید.	
۳۷	**مدیریت مشخصه های امنیتی 1**
محصول می تواند با اعمال تعیین سطح دسترسی بر اساس نقش ، توانایی تغییر پیش‌فرض، پرس و جو، تغییر، حذف، ایجاد مشخصه‌های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود نماید.	
۳۸	**مدیریت مشخصه های امنیتی ۳**
محصول برای مشخصه‌های امنیتی که برای اعمال خط مشی استفاده می‌شوند، می تواند مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.	
۳۹	**مدیریت مشخصه های امنیتی ۴**

شماره الزام	نام الزام
محصول برای تعیین مقادیر اولیه پیشنهادی می تواند به مدیر سیستم اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد.	
۴۰	**مدیریت داده های محصول ۱-مدیر سیستم**
محصول می تواند توانایی تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم محدود نماید.	
۴۱	**مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده**
محصول می تواند توانایی تغییر پیش‌فرض، پرس‌وجو، تغییر پسورد به کاربر عادی محدود نماید.	
۴۲	**کارکردهای مدیریتی محصول ۱**

محصول می تواند قادر به انجام کارکردهای مدیریتی زیر باشد:

مولفه	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
ذخیره سازی رویدادهای ممیزی ۷	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی ۱	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
ورود داده های کاربری به محصول ۴	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق ۱	مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت 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
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۱	مدیر مجاز می‌تواند مقادیر مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و یا تغییر دهد.
مدیریت مشخصه‌های امنیتی 1	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
مدیریت مشخصه های امنیتی ۳	• مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. • نقش مدیر سیستم توانایی مشخص نمودن مقادیر اولیه را داراست. • مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
مدیریت داده های محصول ۱- مدیر سیستم	مدیریت گروهی از قوانین مرتبط با داده‌های محصول
مدیریت داده های محصول ۱- کاربرعادی، وارد کننده داده	مدیریت گروهی از قوانین مرتبط با داده‌های محصول **توضیح:** کاربر عادی نمی تواند قوانین مرتبط با داده های محصول را مدیریت کند. چون در فرآیند آموزش کاربرعادی نباید این امکان را داشته باشد.

شماره الزام	نام الزام

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 به طور همزمان توسط مدیر **توضیح:** در ماژول یادگیری الکترونیکی با توجه به اینکه نشست های همزمان یک کاربر در آن واحد ممکن است موجب سوء استفاده گردد، نشست های فعال کاربر محدود به یک نشست می باشد اما با توجه به ماهیت کسب و کار سایر ماژول ها این مکانیسم حساسیت برانگیز نمی باشد.
قفل کردن و خاتمه دادن به نشست ها ۵	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.

۴۳	**نقش های امنیتی ۱**

نقش‌های زیر در محصول باید تعریف شده باشد:

نقش های کاربری به تفکیک ماژول های سیستم

- **نرم افزار مدیریت اموزش**
  - مدیر سیستم
  - مدیر استانی
- **نرم افزار سامانه فراگیر**
  - فراگیر
  - مدرس
- **نرم افزار یادگیری الکترونیکی**
  - مدیر سیستم
  - فراگیر

مدرس

۴۴	**نقش‌های امنیتی ۲**

محصول، قادر به مرتبط نمودن کاربران با نقش‌های مجاز تعریف شده می باشد.

۴۵	**لغو مشخصه های امنیتی ۱**

محصول می تواند توانایی لغو نام کاربری مربوط به موجودیت‌های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود نماید.

۵,۶ کلاس حفاظت از توابع امنیتی محصول

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

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

شماره الزام	عنصر امنیتی
شکست‌های نرم‌افزاری، سخت افزاری و شبکه ای **توضیح:** در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند.	
۴۷	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۱**
محصول در صورت استفاده از محصولات امن IT، می تواند تفسیر سازگار ممیزی، شناسه کاربری و رمز عبور را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. توضیح: اشتراک‌گذاری داده‌های امنیتی بین محصول و دیگر محصولات امن IT از طریق مکانیسم احراز هویت مرکزی با استفاده از روش هایی نظیر Active Directory و احراز هویت مرکزی CAS در سازمان مشتری انجام می گیرد.	
۴۸	**انتقال داده امنیتی در داخل محصول ۱**
محصول می تواند هنگام انتقال داده‌ها بین بخش‌های مجزای خود، در برابر افشاء یا تغییر محافظت نماید.	
۴۹	**مهرهای زمانی ۱**
محصول، می تواند قادر به ایجاد مهره‌های زمانی قابل اطمینان باشند.	

۵,۷ کلاس دسترسی به محصول

شماره الزام	نام خانواده	عنصر امنیتی
۵۰	**محدودیت بر روی چندین نشست همزمان ۱**	
محصول می تواند حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.		
۵۱	**محدودیت بر روی چندین نشست همزمان ۲**	
محصول می تواند به صورت پیش‌فرض، یک نشست برای هر کاربر در نظر بگیرد.		
۵۲	**قفل کردن و خاتمه دادن به نشست ها ۵**	
محصول می تواند کلیه نشست‌های تعاملی راه دور[۱] را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد.		
۵۳	**قفل کردن و خاتمه دادن به نشست ها ۶**	
محصول می تواند اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.		
۵۴	**سوابق دسترسی به محصول ۱**	
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست براساس روز، زمان می باشد.		

۵,۸ کلاس کانال‌ها/مسیرهای مورد اعتماد

برای این کلاس، تعدادی الزام مبتنی بر انتخاب در پیوست الف ارائه شده است.

[۱] Remote

شماره الزام	نام الزام
۵۵	**کانال امن ۱**
محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احرازهویت که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۵۶	**کانال امن ۲**
محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۵۷	**کانال امن ۳**
محصول مورد ارزیابی می تواند ارتباطات را از طریق کانال امن، برای **سرویس‌دهی به کاربران** راه‌اندازی نماید.	
۵۸	**مسیر امن ۱**
محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS برای ایجاد کانال ارتباطی امن بین خود و مدیر سیستم راه دور را داشته که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۵۹	**مسیر امن ۲**
محصول مورد ارزیابی می تواند به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۶۰	**مسیر امن ۳**
محصول مورد ارزیابی می تواند استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی کند.	

۵,۹ به‌روزرسانی امن

شماره الزام	نام الزام
۶۱	**به روز رسانی امن ۲**
محصول مورد ارزیابی می تواند این امکان را برای مدیر سیستم امنیتی فراهم کندکه به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را به صورت دستی آغاز نماید و از هیچ مکانیسم به‌روزرسانی دیگری پشتیبانی نکند.	
۶۲	**به روز رسانی امن ۳**
محصول مورد ارزیابی می‌تواند در صورت استفاده از به روز رسانی به روش خودکار، پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از **درهم‌ساز منتشرشده،** ابزاری را برای احراز هویت میان‌افزارآن‌ها در اختیار محصول مورد ارزیابی قرار دهد.	

۶ الزامات تضمین امنیت

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	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۶,۱ کلاس توسعه

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2D)** **شرح مولفه:** توسعه دهنده 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 ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [۲] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۳] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱

[۲]-SFR-enforcing TSFI
[۳]-SFR-supporting TSFI

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مولفه: (ADV_FSP.1.2C) **شرح مولفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.3C)** **شرح مولفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.4C)** **شرح مولفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2E)** **شرح مولفه:** 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»، «تست» و «آسیب‌پذیری» ارائه شده است.

۶,۲ کلاس راهنمای کاربر

۶,۲,۱ راهنمای کاربردی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1D)** **شرح مولفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1C)** **شرح مولفه:** 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 مولفه: (AGD_OPE.1.2C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.3C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.4C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع 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 مولفه: (AGD_OPE.1.5C)** **شرح مولفه:** 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 مولفه: (AGD_OPE.1.6C)** **شرح مولفه:** 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 داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.7C)** **شرح مولفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

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

۶,۲,۲ راهنمای آماده‌سازی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

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

مولفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مولفه: (AGD_PRE.1.2E)** **شرح مولفه:**

مولفه‌های اقدامات ارزیاب	
	ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.

۶,۳ کلاس تست

۶,۳,۱ تست مستقل

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

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

مولفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: تست مستقل ۱ **شماره مولفه: (ATE_IND.1.2E)** **شرح مولفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۶,۴ کلاس آسیب‌پذیری

۶,۴,۱ تحلیل آسیب‌پذیری

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارئه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.1.1C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

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

۶,۵ کلاس پشتیبانی از چرخه حیات

۶,۵,۱ قابلیت‌های پیکربندی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1C)** **شرح مولفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۶,۵,۲ حوزه پیکربندی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.1.1D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

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

۷ شرح خلاصه محصول:

نسخه ۱,۱ سند هدف امنیتی سیستم ... توسط کمیته توسعه X تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

- محصول می تواند برای تمام رویدادهای ورود و خروج کاربر به/ از سیستم، کنترل دسترسی، مشخصه های امنیتی و دیگر رویدادهای قابل ممیزی رکورد ممیزی تولید نماید و برای هر رکورد ممیزی، حداقل اطلاعات تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد، نوع کاربری، IP کاربر، محل خدمت کاربر زیر را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند.
- محصول دارای قابلیت خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش، حذف و ایجاد آیتم جدید، صدور مجوز و گواهینامه، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم و دارای قابلیت نمایش رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر می‌باشد و می‌تواند از خواندن رکوردهای ممیزی توسط کاربران غیر مجاز جلوگیری کرده و امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس مرکز برگزار کننده، کاربر، نوع کاربری، تاریخ، موضوع و نوع رخداد(عملیات) مرتب نماید.
- از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد. کاربر تنها در صورتی امکان حذف داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات حذف را انجام دهد که در آن حالت عملیات پیش گفته در پایگاه داده به طور خودکار ممیزی می شود. در صورت تجاوز دنباله ممیزی از مقدار حجم تعریف شده اولیه می‌تواند حجم مورد نظر را به صورت خودکار و مقداری که از پیش تعیین شده افزایش دهد. در صورت درخواست سازمان طرف قرار داد می توان MailServer برای پایگاه داده تعریف کرد که اگر حجم درایو کمتر از ۱۰۰ مگابایت (یا حجم مشخص دیگری) باقیمانده بود ایمیلی مبنی بر عدم وجود حجم کافی برای ذخیره سازی داده ممیزی به مدیر سیستم ارسال شود.
- می توان بر اساس مشخصه های شعبه، گروه کاربری، محدوده زمانی، موضوع، فرم و IP مجموعه از رویدادها را جهت ممیزی نمودن انتخاب نمود.
- محصول می تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد " استفاده از طرح RSA با اندازه کلید ۲۰۴۸ بیت یا بیشتر که از اسناد FIPS PUB ۱۸۶-۴، "Digital Signature Standard (DSS)"، Appendix B. ۳." پیروی می‌کند تولید کنند و رمزنگاری و رمزگشایی را مطابق با الگوریتم رمزنگاری متقارن AES Key Wrap with Padding (KWP) مطابق سند NIST SP ۸۰۰-۳۸F، با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.
- می توان با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد.
- محصول باید مشخصه‌های امنیتی شناسه کاربر داده های احراز هویت، نقش کاربر، وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)، IP کاربر، رمز عبور کاربر و ایمیل کاربر را برای هر کاربر نگهداری نماید.
- می توان قبل از وارد کردن نام کاربری و گذرواژه از امکان بازیابی رمز عبور استفاده کرده و هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نمود و اقدامات دریافت نام کاربری و کلمه عبور و احراز هویت از طریق Active Directory را برای احرازهویت کاربر فراهم آورد.
- محصول می تواند مشخصه های امنیتی شناسه کاربر، نقش های کاربر، جزئیات واسط کلاینت (مرورگر ، IP)، پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق) تا ۳۰ دقیقه گذشته، پیشینه دسترسی به سند/رکورد اخیر(ممیزی)، کد ملی کاربر و ایمیل کاربر را برای کاربر فعال نگهداری نماید.
  - زمانیکه یک نشست جدید برقرار می شود، اطلاعات موجود از نشست های قبلی حذف می‌گردد. اطلاعات پیشینه احراز هویت بروزرسانی می‌شود. رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید ثبت می‌گردد.

- محصول می تواند هنگام دریافت داده کاربری حداکثر حجم تصویر، فرمت های مجازکد ملی ۱۰ رقمی صحیح را اعمال کرده و از مشخصه های امنیتی مرتبط با داده های کاربری را هنگام ورود داده ها استفاده نماید.
- محصول می‌تواند هنگام خروج داده کاربری به بیرون داده ها را در سه فرمت (pdf,word, Excel) نمایش داده و از خروج داده های حساس مانند نام کاربری و کلمه عبور و ایمیل کاربر جلوگیری کند. امکان نگهداری داده کاربری حساس ذخیره شده در مکان تحت کنترل براساس مشخصه های رمزنگاری امن نگهداری کرده و آنها را به منظور شناسایی خطای صحت داده رکورد و داده ممیزی پایش کند.
- سیستم می تواند هنگام تشخیص خطای صحت داده ممیزی مربوطه را ثبت نماید.
- محصول می تواند دسترسی بر اساس نوع کاربری که بر اساس نقش های کاربر مشخص می شود را بر روی عملیات های مانند ایجاد، تغییر، ویرایش و حذف موجودیت های فعال و غیرفعال اعمال نماید.
- محصول می تواند سطح دسترسی را با توجه به هویت کاربر، نقش ها و مجوزهای کاربر مجاز و اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند، بر روی موجودیت های غیرفعال اعمال نماید.
- سیستم دارای قابلیت محدودسازی توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر می باشد.
- می توان با اعمال تعیین سطح دسترسی بر اساس نقش ، توانایی تغییر پیش‌فرض، پرس و جو، تغییر، حذف، ایجاد مشخصه های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود نمود و امکان در نظرگرفتن مقادیر پیش فرض محدود شده محصول برای مشخصه های امنیتی که برای اعمال خط مشی استفاده می شوند، وجود داشته و مدیر سیستم از طریق فایل Config می تواند هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد.
- محصول می تواند توانایی تغییر پیش‌فرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم و توانایی تغییر پیش‌فرض، پرس و جو، تغییر پسورد به کاربر عادی محدود نماید.
- محصول می تواند به انجام کارکردهای می باشد و می توان در هر یک از ماژول های سیستم نقش های مورد نیاز را تعریف نمود.
- سیستم می تواند کاربران را با نقش‌های مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود کند.
- در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند.
- اشتراک گذاری داده های امنیتی بین محصول و دیگر محصولات امن IT از طریق مکانیسم احراز هویت مرکزی با استفاده از روش هایی نظیر Active Directory و احراز هویت مرکزی CAS در سازمان مشتری انجام می گیرد.
- محصول می تواند هنگام انتقال داده ها بین بخشهای مجزای خود، از آنها در برابر افشاء یا تغییر محافظت نماید.
- محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می باشد.
- محصول می تواند کلیه نشست های تعاملی راه دور را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد و اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.
- در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست براساس روز، زمان می باشد.
- محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احرازهویت که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و

تغییرات را تشخیص دهد. همچنین محصول می تواند اجازه داشته باشد به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند و تمامی بخش های سیستم, سازگاری کامل با پروتکل های امن SSL و غیره را دارند.