به نام خدا

سند هدف امنیتی

پورتال تتیس-۱٫۱٫۵

آرمان دنیای فناوری اطلاعات تتیس

نسخه ۱٫۷

فهرست

۱ معرفی سند هدف امنیتی

۱٫۱ مرجع سند هدف امنیتی و هدف ارزیابی

عنوان سند هدف امنیتی	سند هدف امنیتی پورتال تتیس
نسخه	۱٫۷
تاریخ	مهر ۱۳۹۸
نویسندگان	واحد توسعه شرکت آرمان دنیای فناوری اطلاعات تتیس

نام تولید کننده (شرکت)	شرکت آرمان دنیای فناوری اطلاعات تتیس
نام محصول	پورتال تتیس
نوع محصول	سامانه مدیریت محتوا / پورتال
نسخه	۵٫۱٫۱

۱٫۲ مرور کلی هدف ارزیابی

- **موارد استفاده هدف ارزیابی**

نرم افزار پورتال تتیس یک سیستم مدیریت محتوا با امکان تعریف وب سایت، مدیریت صفحات، طراحی صفحه و ورود اطلاعات جهت راه اندازی سایت ها و پورتال های اطلاع رسانی می باشد و به عنوان سایت اطلاع رسانی یک سازمان مورد استفاده قرار می گیرد .

- **توابع امنیتی اصلی هدف ارزیابی**

- مدیریت کاربران
- مدیریت نقش ها و گروه ها
- ممیزی کاربران و اطلاعات
- مدیریت گذرواژه
- مدیریت سطح دسترسی
- احراز هویت کاربران

- **نوع هدف ارزیابی**

- **نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی**

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

کامپوننت‌ها	حداقل الزامات
پردازنده	Intel Dual Xeon Processor (2.8 GHz +, 6-core, 12 Mb Cache)
فضای آزاد دیسک	300 GB
حافظه	32 GB +
سیستم عامل	Windows Server 2016
پایگاه داده	SQL Server 2014 R2 + (2017 Recommended)
سایر نرم افزارها	IIS 10 .NET Framework 4.7 Browser: IE 11, Edge, Chrome, Firefox

۱٫۳ توصیف هدف ارزیابی

نرم افزار پورتال تتیس یک سیستم مدیریت محتوا با امکان تعریف وب سایت، مدیریت صفحات، طراحی صفحه و ورود اطلاعات می باشد .

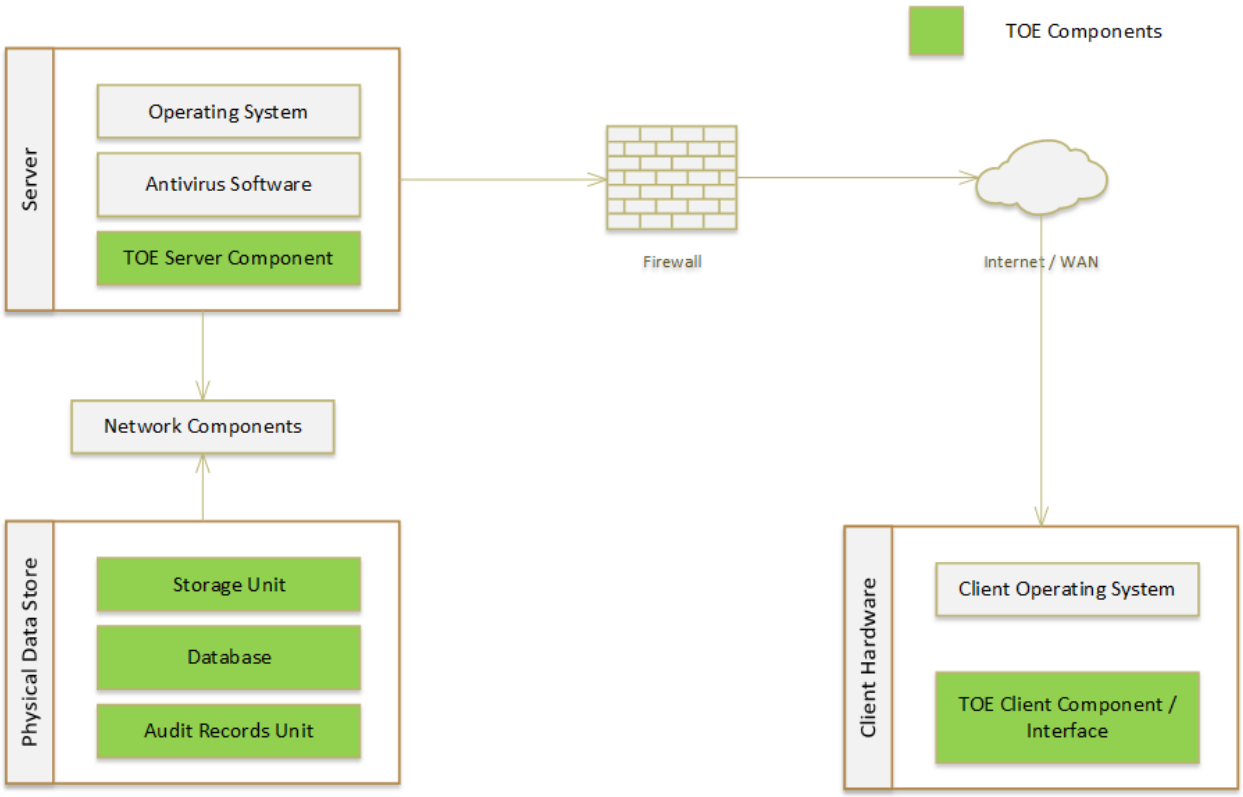
این نرم افزار دارای امکاناتی نظیر احراز هویت کاربران، اعمال سطوح دسترسی، ثبت، ویرایش و حذف رکوردها، مدیریت کاربران و گروه ها و امکان نمایش و جستجوی اطلاعات می باشد.

- **حوزه فیزیکی**

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر هدف ارزیابی	شماره مدل یا نسخه
نرم افزار پورتال تتیس	نسخه ۵٫۱٫۱

در این بخش قرار گیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شده است.



- **حوزه منطقی**

کارکردها	توصیف
احراز هویت کاربران	*امکان احراز هویت کاربر از طریق خود نرم افزار (مبتنی بر فرم) و یا از طریق ویندوز و یا Active Directory وجود دارد*
اعطای حق دسترسی	*امکان اعطای حقوق دسترسی به کاربران یا گروه ها وجود دارد*
کنترل دسترسی	*امکان کنترل دسترسی کاربران به صورت مستقل یا با توجه به گروه هایی که عضو آن است به بخش های مختلف نرم افزار از جمله سایت ها، صفحات، دسته بندی های اطلاعات و رکوردهای اطلاعاتی وجود دارد*
مدیریت امنیت	*امکان تغییر تنظیمات امنیتی نرم افزار وجود دارد*
مدیریت کاربران و گروه ها	*امکان تعریف کاربران و گروه ها در نرم افزار وجود دارد*

رویداد نگاری	*امکان رویداد نگاری از عملکرد کاربران در سیستم برای عملیاتی مانند ورود به سیستم، خروج از سیستم، ثبت رکورد، ویرایش رکورد، حذف رکورد وجود دارد*
صحت رکوردها	*صحت رکوردهای اطلاعاتی وارد شده توسط کاربر توسط سیستم چک می شود تا از خارج از نرم افزار تغییر نکرده باشد. صحت اطلاعات سامانه، صحت مشخصات کاربران و صحت رکوردهای ممیزی توسط نرم افزار بررسی و تایید می گردند.*
پشتیبان گیری	*انجام عملیات پشتیبان گیری در بازه های زمانی مشخص. این عملیات از طریق تنظیمات سرور پایگاه داده (SQL Agent) بر روی سرور قابل انجام می باشد.*
درهم سازی / رمز نمودن داده های حساس	*اطلاعات حساسی مشابه گذرواژه کاربران در سیستم به صورت رمز شده و یا درهم سازی شده ذخیره می گردد.*

۲ ادعای انطباق

۲٫۱ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	*ISO/IEC 15408 V3.1 R4*
نوع انطباق با بخش دوم استاندارد (SFRها)	*توسعه یافته*
نوع انطباق با بخش سوم استاندارد (SARها)	*منطبق*
نام پروفایل حفاظتی	منطبق با پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه منتشر شده توسط مرکز مدیریت راهبردی افتا نسخه ۱٫۱
سطح تضمین امنیتی	*EAL1*

۳ تعریف مسائل امنیتی

۳٫۱ خطمشی

خطمشی‌ها	توصیف
ممیزی کامل P.COMPLEMENTARY_AUDIT	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.
پیکربندی مناسب P.PROPER_CONFIGURATION	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. سرویس-هایی 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 P.E_SIGNATURE	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳٫۲ تهدیدات

تهدید	توصیف
دسترسی غیرمجاز T.UNAUTHORIZED_ACCESS	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده هویت

تهدید	توصیف
	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 T.DATA_ALTERATION	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 T.REPUDIATION	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.

تهدید	توصیف
افشای اطلاعات T.DATA_DISCLOSURE	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 T.DENIAL_OF_SERVICE	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 T.HARMFUL_DATA	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 T.ELEVATION_OF_PRIVILEGES	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 T.NETWORK_SNIFFING	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد موردنظر را مورد

تهدید	توصیف
	نظارت قرار دهد. این حمله شامل نظارت بر داده‌های رد و بدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان 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.

۳٫۳ فرضیات

فرضیات	*توصیف*
کاربران آموزش دیده A.TRUSTED_ADMIN	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می-نمایند.
توسعه دهندگان آموزش دیده A.TRUSTED_DEVELOPER	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 A.EXPERIENCED_DEVELOPER	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 A.SECURE_ENVIRONMENT	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.

فرضیات	توصیف
پشتیبان گیری مناسب A.PROPER_BACKUP	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 A.COMMUNICATION	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.
تحویل امن A.SECURE_DELIVERY	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 A.DIST_DENIAL_OF_SERVICE	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

٤ اهداف امنیتی

۴٫۱ اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
ممیزی O.AUDIT	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.

هدف امنیتی	توصیف
احراز هویت O.AUTH	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 O.DATA_FLOW_CONTROL	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 O.DATA_INTEGRITY	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با

هدف امنیتی	توصیف
	تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت O.MANAGEMENT	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.
مدیریت خطا O.ERROR_MANAGEMENT	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 صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده‌های باقیمانده O.RESIDUAL_DATA_MNG	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.
ارتباطات امن مبتنی بر TLS O.TLS_COMMUNICATION	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۴,۲ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
محیط امن OE.SECURE_ENVIRONMENT	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 OE.COMMUNICATION	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه-های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده OE.TRUSTED_ADMIN	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 OE.TRUSTED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان مجرب OE.EXPERIENCED_DEVELOPER	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 OE.COMPLEMENTARY_AUDIT	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می-گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط

هدف امنیتی	توصیف
	عملیاتی محصول می‌باشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن OE.SECURE_DELIVERY	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.
پشتیبان‌گیری مناسب OE.PROPER_BACKUP	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 که مطابق پروفایل حفاظتی تهیه گردیده است. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند. برای انتخاب از Underline استفاده شده و برای اختصاص از Bold استفاده شده است.

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
٤	**بازبینی داده ممیزی ۱**	FAU_SAR.1.1
۵	**بازبینی داده ممیزی ۲**	FAU_SAR.1.2
٦	**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

شماره الزام	نام الزام	تطابق الزام با استاندارد
۹	**ذخیره سازی رویدادهای ممیزی ۲**	FAU_STG.1.2
۱۰	**ذخیره سازی رویدادهای ممیزی ٦**	FAU_STG.3.1
۱۱	**ذخیره سازی رویدادهای ممیزی ۷**	FAU_STG.4.1
۱۲	**انتخاب داده ممیزی ۱**	FAU_SEL.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	**الزامات پروتکل TLS Client (۱)**	FCS_TLSC_EXT.1.1
۱٦	**الزامات پروتکل TLS Client (۲)**	FCS_TLSC_EXT.1.2
۱۷	**الزامات پروتکل TLS Client (۳)**	FCS_TLSC_EXT.1.3
۱۸	**الزامات پروتکل TLS Client (۴)**	FCS_TLSC_EXT.4.1
۱۹	**مدیریت کلمه عبور**	FIA_PMG_EXT.1.1
۲۰	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
۲۱	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
۲۲	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۲۳	**شناسایی کاربر ۱**	FIA_UID.1.1
۲۴	**شناسایی کاربر ۲**	FIA_UID.1.2
۲۵	**احراز هویت کاربر ۱**	FIA_UAU.1.1
۲٦	**احراز هویت کاربر ۲**	FIA_UAU.1.2
۲۷	**احرازهویت کاربر ۷**	FIA_UAU.5.1
۲۸	**احرازهویت کاربر ۸**	FIA_UAU.5.2
۲۹	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱**	FIA_USB.1.1
۳۰	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲**	FIA_USB.1.2
۳۱	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**	FIA_USB.1.3
۳۲	**الزامات پروتکل X509 (۱)**	FIA_X509_EXT.1.1
۳۳	**الزامات پروتکل X509 (۲)**	FIA_X509_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۴	**الزامات پروتکل X509 (۳)**	FIA_X509_EXT.2.1
۳۵	**الزامات پروتکل X509 (۴)**	FIA_X509_EXT.2.2
۳٦	**حفاظت از اطلاعات باقیمانده در منابع ۲**	FDP_RIP.2.1
۳۷	**صحت داده های کاربری ذخیره شده ۲**	FDP_SDI.2.1
۳۸	**صحت داده های کاربری ذخیره شده ۳**	FDP_SDI.2.2
۳۹	**خط مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۴۰	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۴۱	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۴۲	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۴۳	**عملیات کنترل دسترسی ۴**	FDP_ACF.1.4
۴۴	**مدیریت کارکرد در محصول ۱**	FMT_MOF.1.1
۴۵	**مدیریت مشخصه‌های امنیتی ۱**	FMT_MSA.1.1
۴٦	**مدیریت مشخصه های امنیتی ۳**	FMT_MSA.3.1
۴۷	**مدیریت مشخصه های امنیتی ۴**	FMT_MSA.3.2
۴۸	**مدیریت داده های محصول ۱-مدیر سیستم**	FMT_MTD.1.1(1)
۴۹	**مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده**	FMT_MTD.1.1(2)
۵۰	**کارکردهای مدیریتی محصول ۱**	FMT_SMF.1.1
۵۱	**نقش‌های امنیتی ۱**	FMT_SMR.1.1
۵۲	**نقش‌های امنیتی ۲**	FMT_SMR.1.2
۵۳	**حفظ وضعیت امن در زمان شکست ۱**	FPT_FLS.1.1
۵۴	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۱**	FPT_TDC.1.1
۵۵	**سازگاری داده های امنیتی بین محصول و موجودیت امن۲**	FPT_TDC.1.2
۵٦	**انتقال داده امنیتی در داخل محصول ۱**	FPT_ITT.1.1
۵۷	**مهرهای زمانی ۱**	FPT_STM.1.1
۵۸	**به روز رسانی امن ۲**	FPT_TUD_EXT.1.2
۵۹	**محدودیت بر روی چندین نشست همزمان ۱**	FTA_MCS.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
٦٠	محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
٦١	قفل کردن و خاتمه دادن به نشست ها ۵	FTA_SSL.3.1
٦٢	قفل کردن و خاتمه دادن به نشست ها ٦	FTA_SSL.4.1
٦٣	سوابق دسترسی به محصول ۱	FTA_TAH.1.1
٦٤	سوابق دسترسی به محصول ۲	FTA_TAH.1.2
٦٥	سوابق دسترسی به محصول ۳	FTA_TAH.1.3
٦٦	برقراری نشست ۱	FTA_TSE.1.1
٦٧	کانال امن ۱	FTP_ITC.1.1
٦٨	کانال امن ۲	FTP_ITC.1.2
٦٩	کانال امن ۳	FTP_ITC.1.3
٧٠	مسیر امن ۱	FTP_TRP.1.1
٧١	مسیر امن ۲	FTP_TRP.1.2
٧٢	مسیر امن ۳	FTP_TRP.1.3
٧٣	تحمل خطا ۱	FRU_FLT.1.1
	توجیهات	
٧٤	تولید کلید رمزنگاری ۱	FCS_CKM.1.1
٧٥	مدیریت کلید رمزنگاری ۱	FCS_CKM_EXT.4.1
٧٦	الزامات پروتکلTLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
٧٧	الزامات پروتکلTLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
٧٨	الزامات پروتکلTLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
٧٩	ورود داده های کاربری به محصول ۴	FDP_ITC.2.1
٨٠	ورود داده های کاربری به محصول ۵	FDP_ITC.2.2
٨١	ورود داده های کاربری به محصول ٦	FDP_ITC.2.3
٨٢	ورود داده های کاربری به محصول ۷	FDP_ITC.2.4
٨٣	ورود داده های کاربری به محصول ۸	FDP_ITC.2.5
٨۴	خروج داده های کاربری از محصول ۳	FDP_ETC.2.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۸۵	**خروج داده های کاربری از محصول ۴**	FDP_ETC.2.2
۸٦	**خروج داده های کاربری از محصول ۵**	FDP_ETC.2.3
۸۷	**خروج داده های کاربری از محصول ٦**	FDP_ETC.2.4
۸۸	**مهرهای زمانی ۱**	FPT_STM.1.1
۸۹	**به روز رسانی امن ۳**	FPT_TUD_EXT.1.3

۵,۱ کلاس ممیزی امنیت

شماره الزام	عنصر امنیتی
۱	**تولید داده ممیزی ۱ -** FAU_GEN.1.1

محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:

- آغاز و اتمام توابع ممیزی؛
- رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول ۱ آمده است.

ردیف	مولفه	رویداد قابل ممیزي	جزئیات
۱	FAU_SAR.1	(Minimal)خواندن اطلاعات از رکوردهاي ممیزي	
۲	FAU_SAR.2	(Minimal) تلاش‌هاي ناموفق براي خواندن اطلاعات از رکوردهاي ممیزي	
۳	FAU_SEL.1	(Minimal) تغییرات انجام شده بر روي تنظیمات ممیزي در حالیکه تابع ممیزي فعال است.	
٤	FAU_STG.3	(Minimal) عملیاتي که در هنگام عبور از حد آستانه تابع ممیزي روي میدهد.	
٥	FAU_STG.4	(Minimal) عملیات انجام شده به دلیل شکست ذخیره سازي ممیزي	
٦	FCS_COP.1(1)	• (Minimal) موفقیت یا شکست، و نوع عملیات رمزنگاري • (basic) هر مد عملیاتي قابل اعمال رمزنگاري، ویژگي هاي موجودیت فعال و غیرفعال	
۷	FCS_COP.1(2)	• (Minimal) موفقیت یا شکست، و نوع عملیات رمزنگاري	

		• (basic) هر مد عملياتي قابل اعمال رمزنگاري، ويژگي هاي موجوديت فعال و غيرفعال	
۸	FDP_ACF.1	(Minimal) درخواست هاي موفق براي اجراي عمليات بر روي يک موجوديت غيرفعال تحت پوشش سياست توابع امنيتي (basic) تمامي درخواست‌هاي موفق و ناموفق براي اجراي عمليات بر روي يک موجوديت غيرفعال محصول	شناسايي داده هاي موجوديت غيرفعال
۹	FDP_ITC.2	(Minimal) ورود موفق داده كاربري، شامل هر مشخصه هاي امنيتي (basic) همه تلاش ها براي ورود داده كاربر، شامل هر مشخصه هاي امنيتي	
۱۰	FDP_ETC.2	(Minimal) خروج موفق اطلاعات (basic) همه تلاش ها براي خروج اطلاعات	
۱۱	FDP_SDI.2	• (Minimal) تلاش هاي موفق براي بررسي صحت داده كاربر، شامل يک نشانه از نتايج بررسي • (basic) همه تلاش ها براي بررسي صحت داده كاربر، شامل يک نشانه از نتايج بررسي اگر انجام شده باشد.	
۱۲	FIA_AFL.1	(Minimal) رسيدن به حد آستانه براي تلاش هاي احرازهويت ناموفق و اقداماتي (براي مثال غيرفعال كردن ترمينال) كه انجام ميشود و عواقب اگر مناسب بود، برگرداندن سامانه به وضعيت عادي (براي مثال فعال سازي مجدد يک ترمينال)	
۱۳	FIA_UAU.1	•(Minimal) استفاده ناموفق از مكانيزم	

		احرازهویت •(basic) همه استفاده ها از مکانیزم احرازهویت	
١٤	FIA_UAU.5	•(Minimal) آخرین تصمیم براي احرازهویت •(basic) نتیجه هر مکانیزم فعال شده همراه با تصمیم نهایي	
١٥	FIA_UID.1	•(Minimal) استفاده ناموفق از مکانیزم شناسایي کاربر، از جمله هویت کاربران ارائه شده. •(basic) همه استفاده ها از مکانیزم شناسایي کاربر(موفق و ناموفق)، از جمله هویت کاربران ارائه شده.	
١٦	FIA_USB.1	(Minimal) پیوند ناموفق ویژگي هاي امنیتي کاربر با موجودیت فعال (براي مثال ایجاد یک کاربر) (basic) پیوند موفق و ناموفق ویژگي هاي امنیتي کاربر با موجودیت فعال (براي مثال ایجاد موفق یا ناموفق یک کاربر)	
١٧	FMT_MOF.1	(basic) تمامي تغییرات بر روي رفتار توابع امنیتي هدف ارزیابي	
١٨	FMT_MSA.1	(basic) تمامي تغییرات بر روي مقادیر مشخصه-هاي امنیتي	
١٩	FMT_MSA.3	(basic) تغییرات بر روي تنظیمات پیشفرض قوانین محدودکننده و یا مجاز (basic) تمامي تغییرات بر روي مقادیر اولیه مشخصه‌هاي امنیتي	
٢٠	FMT_MTD.1(1)	(basic) تمامي تغییرات بر روي مقادیر داده‌هاي توابع امنیتي	

۲۱	FMT_MTD.1(2)	(basic) تمامي تغييرات بـر روي مقـادير داده‌هـاي توابع امنيتي	
۲۲	FMT_SMF.1	(minimal) استفاده از توابع مديريتي	
۲۳	FMT_SMR.1	(minimal) تغيـيرات بـر روي گروهـي از کـاربران بخشي از يک نقش است	
۲٤	FPT_FLS.1	(basic) شکست توابع امنيتي	
۲۵	FPT_TDC.1	(minimal) موفقيت استفاده از مکانيزم سازگار داده توابع امنيتي. (basic) اسـتفاده از مکـانيزم هـاي سـازگار داده توابع امنيتي	
۲٦	FRU_FLT.1	(minimal) هر شکستي که توسط توابع امنيتي شناسايي ميشود (basic) همه قابليت هاي محصول که به علت شکست متوقف ميشود.	
۲۷	FTA_MCS.1	(minimal) عدم پذيرش يک نشست جديد بر اساس محدوديت چندين نشست هاي همزمان	
۲۸	FTA_SSL.3	(minimal) پايان دادن به يک نشست توسط مکانيزم قفل نشست	
۲۹	FTA_SSL.4	(minimal) پايان دادن به يک نشست توسط کاربر	
۳۰	مديريت کلمه عبور	تلاش موفق و ناموفق ورود کاربر	بـراي مثـال، رد و يـا قبـول کلمـه عبور کاربر

۲	**تولید داده ممیزی ۲** - FAU_GEN.1.2
محصول باید برای هر رکورد ممیزي، 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. **آدرس IP، آدرس Url و SessionID و مشخصات مرورگر کاربر**	
۳	**تولید داده ممیزی ۳** - FAU_GEN.2.1
براي رویدادهاي ممیزي حاصل از اقدامات کاربران شناسایي شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید.	
۴	**بازبینی داده ممیزی ۱** - FAU_SAR.1.1
محصول باید امکان خواندن/مشاهده **همه رکوردهای ممیزی** از کل رکوردهاي ممیزي را برای **کاربران مجاز که دسترسی برای آنها اعطا شده** فراهم نماید.	
۵	**بازبیني داده ممیزي ۲** - FAU_SAR.1.2
محصول باید رکوردهاي ممیزي را به شکل خوانا و قابل درک براي کاربر نمایش دهد.	
٦	**بازبینی داده ممیزی ۳** - FAU_SAR.2.1
محصول باید از دسترسي کلیه کاربران بجز کاربرانی که به آنها مجوز دسترسي خواندن داده شده باشد (الزام شماره ۴) جهت خواندن رکوردهاي ممیزي ممانعت نماید.	
۷	**بازبینی داده ممیزی ۴** - FAU_SAR.3.1
محصول باید امکان انجام **انتخاب و مرتب سازی** رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس **حساب کاربری، تاریخ/زمان، مکان، نوع رخداد** مرتب نماید. با توجه به اینکه درجه اهمیت در سیستم ذخیره نمی شود امکان مرتب سازی بر آن اساس وجود ندارد، همچنین چون تمام کاربران از طریق وب به نرم افزار متصل می شوند روش اتصال برای کاربر ذخیره نمی شود (در صورتیکه منظور نوع مرورگر کاربر نباشد) برای مکان نیز صرفا آدرس IP کاربر ذخیره می شود.	

۸	**ذخیره سازی رویدادهای ممیزی ۱** - FAU_STG.1.1
محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت نماید.	
۹	**ذخیره سازی رویدادهای ممیزی ۲** - FAU_STG.1.2
محصول باید قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در محل ذخیره سازی آنها باشد.	
۱۰	**ذخیره سازی رویدادهای ممیزی ٦** - FAU_STG.3.1
محصول در صورت تجاوز دنباله ممیزی از **حد آستانه تعیین شده** باید با استفاده از **طریق واسطهای محصول و همچنین از طریق ایمیل** کاربران مربوطه را مطلع نماید.	
۱۱	**ذخیره سازی رویدادهای ممیزی ۷** - FAU_STG.4.1
محصول در صورت پر شدن دنباله ممیزی، باید « روی قدیمیترین رکوردهای ممیزی ذخیرهشده دوبارهنویسی نماید ». و یک هشدار ارسال نماید.	
۱۲	**انتخاب داده ممیزی ۱** - FAU_SEL.1.1
محصول باید قادر به انتخاب مجموعهای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصههای زیر باشد: • هویت موجودیت فعال، نوع رخداد • **هیچ معیار دیگری**	

۵,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	عنصر امنیتی
۱۳	**عملیات رمزنگاری ۱ (۱) (یکپارچگي دادههاي رکورد و دادههاي ممیزي)** - FCS_COP.1.1(1)
توابع امنیتی هدف ارزیابی باید **برای وارسی صحت داده های ممیزی و داده های رکورد** بر اساس یک الگوریتم رمزنگاری مشخص **SHA-256 مطابق مستند NIST FIPS PUB 180-4,** و اندازه کلید رمزنگاری **۲۵٦** اجرا شود که مطابق با **SHA-256 Hash Computation مطابق سند NIST FIPS PUB 180-4** باشد.	
۱۴	**عملیات رمزنگاری ۱(۲) (تولید مقادیر Hash)** - FCS_COP.1.1(2)
محصول باید **تولید داده درهمسازی** به منظور بررسی صحت اطلاعات کاربر را بر اساس الگوریتم رمزنگاری **SHA-256** که مطابق با **NISI FIPS PUB 180-4** باشد اجرا نماید.	

۱۵	**الزامات پروتکل TLS Client (۱)** - FCS_TLSC_EXT.1.1
محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: ○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289	
۱٦	**الزامات پروتکل TLS Client (۲)** - FCS_TLSC_EXT.1.2
محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ٦ از RFC 6125، تأیید نماید.	
۱۷	**الزامات پروتکل TLS Client (۳)** - FCS_TLSC_EXT.1.3
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید ارتباط را برقرار نسازد، **در صورتیکه مدیر سیستم تنظیمات لازم را انجام داده باشد برای برقراری ارتباط اجازه بدهد.**	
۱۸	**الزامات پروتکل TLS Client (۴)** - FCS_TLSC_EXT.4.1
محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های secp256r1, secp384r1 در پیام ClientHello ارائه دهد.	

۵,۳ کلاس شناسایی و احرازهویت

شماره الزام	عنصر امنیتی
۱۹	**مدیریت کلمه عبور ۱** - FIA_PMG_EXT.1.1
محصول باید 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 بوده و ۸ کاراکتر یا بیشتر باشد.	
۲۰	**مدیریت احراز هویت ناموفق ۱** - FIA_AFL.1.1
محصول، باید با استفاده از یک عدد مثبت قابل تنظیم توسط مدیر **بین ۱ تا ۱۰** تلاش ناموفق احراز هویت مرتبط با **تلاش کاربر برای احراز هویت شدن** را تشخیص دهد.	
۲۱	**مدیریت احراز هویت ناموفق ۲** - FIA_AFL.1.2
زماني که تعداد تلاش‌هاي ناموفق صورت گرفته براي احراز هويت به حد تعیین شده رسید ، محصول باید **نسبت قفل کردن حساب کاربری بپردازد** که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.	
۲۲	**تعریف مشخصات کاربر ۱** - FIA_ATD.1.1
محصول باید مشخصه‌هاي امنيتي زير را برای هر کاربر نگهداري نماید: • شناسه کاربر • متد احرازهویت مورد استفاده • داده های احراز هویت • نقش کاربر • وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)	
۲۳	**شناسایی کاربر ۱** - FIA_UID.1.1
محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: • **مشاوره و راهنمایی نحوه ورود به سیستم**	

۲۴	**شناسایی کاربر ۲** - FIA_UID.1.2
محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میاني دیگري از سوي او وجود داشته باشد، با موفقیت شناسایي نماید.	
۲۵	**احراز هویت کاربر ۱**- FIA_UAU.1.1
محصول باید پیش از احراز هویت کاربر، اجازه اقدامات زیر را دهد: • **مشاهده راهنمای نحوه ورود به سیستم**	
۲٦	**احراز هویت کاربر ۲** - FIA_UAU.1.2
محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میاني دیگري از سوي او وجود داشته باشد، احراز هویت نماید.	
۲۷	**احراز هویت کاربر ۷** - FIA_UAU.5.1
محصول باید به منظور احراز هویت کاربر ساز و کارهای زیر را فراهم آورد: • **نام کاربری و کلمه عبور** • **احراز هویت دو مرحله ای (ارسال ایمیل)**	
۲۸	**احراز هویت کاربر ۸** - FIA_UAU.5.2
محصول باید هر کاربر متقاضی احراز هویت را مطابق **نوع کاربر به این صورت که کاربران از راه دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه که در بالا تعریف شده استفاده کند، پس از ورود نام کاربری و کلمه عبور یک کد امنیتی برای آنها ایمیل می شود و کد امنیتی را باید جهت تایید هویت در سیستم وارد نماید تا** احراز هویت نماید.	
۲۹	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱** - FIA_USB.1.1
محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: • **شناسه کاربر** • **نقش‌های و یا مجموعه دسترسی های کاربر به قسمت های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احراز هویت (جزییات تلاش برای احراز هویت موفق و نا موفق)** • **هیچ مشخصه کاربری دیگری**	

۳۰	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲** - FIA_USB.1.2
محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید: • **زمانی که یک نشست جدید برقرار می شود، اعتبار نشست های قبلی باید از بین برود (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد و هنگام فعال شدن نشست دوم و بیشتر در برنامه، باید به صفحه کاربر نشست اصلی(اول) اطلاع داده شود.)** • **اطلاعات پیشینه احراز هویت باید بروزرسانی گردد** • **هیچ قانونی دیگری**	
۳۱	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳** - FIA_USB.1.3
محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: **هیچ تغییر در طول نشست فعال مجاز نمی باشد**	
۳۲	**الزامات پروتکل X509 (۱) / ابطال** - FIA_X509_EXT.1.1/Rev
محصول مورد ارزیابی باید گواهی نامه ها را بر اساس قوانین زیر تایید کند: • تایید گواهی نامه RFC 5280 و تایید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می کند. • مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تایید یک مسیر گواهی نامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه های CA به حالت «True» تنظیم شده است • محصول مورد ارزیابی باید وضعیت فسخ گواهی نامه را با استفاده از هیچ روش فسخ تایید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تایید کند: ○ گواهی نامه های مورد استفاده برای تایید به روز رسانی های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند.	

○ گواهی نامه های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی نامه های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی نامه های OCSP مورد استفاده برای پاسخ های OCSP باید هدف « OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.	
۳۳	**الزامات پروتکل X509 (۲) / ابطال** - FIA_X509_EXT.1.2/Rev
محصول مورد ارزیابی تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی نامه را به عنوان گواهی نامه CA می پذیرد.	
۳۴	**الزامات پروتکل X509 (۳)** - FIA_X509_EXT.2.1
محصول مورد ارزیابی باید جهت پشتیبانی احراز هویت برای TLS و هیچ کاربرد دیگر از گواهی نامه های X509v3 تعریف شده در RFC 5280 استفاده کند.	
۳۵	**الزامات پروتکل X509 (۴)** - FIA_X509_EXT.2.2
هنگامی که محصول مورد ارزیابی نمی تواند ارتباط لازم برای احراز اعتبار گواهی نامه را برقرار کند، محصول مورد ارزیابی باید به مدیر سیستم اجازه قبول گواهی نامه را بدهد.	

۵٫۴ کلاس حفاظت از داده کاربری

شماره الزام	عنصر امنیتی
۳٦	**حفاظت از اطلاعات باقیمانده در منابع ۲** - FDP_RIP.2.1
محصول باید تضمین کند هرگونه محتوی اطلاعات قبلی یک منبع را هنگام تخصیص منابع به تمام موجودیت‌های غیرفعال استفاده شده، غیرقابل دسترس کند.	

۳۷	**صحت داده های کاربری ذخیره شده ۲** - FDP_SDI.2.1
محصول باید داده کاربری ذخیره شده در مکان تحت کنترل خود را برای **خطاهای صحت داده** داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های **درهم شده**[1] **داده‌های کاربری ذخیره شده** پایش نماید.	
۳۸	**صحت داده های کاربری ذخیره شده ۳** - FDP_SDI.2.2
هنگام تشخیص خطای صحت داده، محصول باید **جلوگیری از نمایش رکورد** را صورت دهد.	
۳۹	**خط مشی کنترل دسترسی ۱** - FDP_ACC.1.1

محصول باید **خط‌مشی‌های کنترل دسترسی** را بر روی موارد زیر اعمال نماید:

- موجودیت فعال: **مدیر سیستم، کاربر عادی**
- موجودیت غیرفعال:
  - رکوردها، مستندات و فرا داده
  - داده‌های متعلق به کاربر
  - داده احرازهویت
  - داده ها با این معیارها: **هیچ معیار دیگری**
  - **رکوردهای رویدادنگاری، صفحات**
- عملیات:
  - ایجاد موجودیت غیرفعال جدید
  - حذف موجودیت غیرفعال
  - تغییر دسترسی‌ها به موجودیت غیرفعال
  - عملیات بر روی فرداده‌های وابسته به موجودیت غیرفعال
  - **هیچ عملیات دیگری**

۴۰	**عملیات کنترل دسترسی ۱** - FDP_ACF.1.1
محصول باید **خط‌مشی‌های کنترل دسترسی** را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید:	

[1] Hash

• **هویت کاربر** • **نقش‌ها و مجوزهای کاربر مجاز** • **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند**	
۴۱	**عملیات کنترل دسترسی ۲** - FDP_ACF.1.2
محصول باید 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.**	
۴۲	**عملیات کنترل دسترسی ۳** - FDP_ACF.1.3
محصول باید 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.	
۴۳	**عملیات کنترل دسترسی ۴** - FDP_ACF.1.4
محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری - نماید: • تعداد درخواست‌های بالای ناگهانی از یک یا بیشتر از یک IP مشخص، • تجاوز تعداد تلاش‌های احرازهویت یک کاربر مشخص از مقدار آستانه از پیش تعریف شده، • تعداد درخواست‌های بالای ناگهانی از یک کاربر مجاز، • تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[۲] از پیش تعریف شده،	

[2] Threshold

۵,۵ کلاس مدیریت امنیت

شماره الزام	عنصر امنیتی
۴۴	**مدیریت کارکرد در محصول ۱** - FMT_MOF.1.1
محصول باید توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار کارکرد **تمام کارکردهای مربوط به مدیریت محصول** را به **مدیر سیستم یا دیگر نقش‌ها** محدود نماید.	
۴۵	**مدیریت مشخصه های امنیتی ۱** - FMT_MSA.1.1
محصول باید با اعمال **خط‌مشی کنترل دسترسی**، توانایی تغییر پیش‌فرض، پرس و جو، تغییر، حذف مشخصه‌های امنیتی و **مجوزهایی که کاربران بر روی اطلاعات وجود دارد سیستم داده می شود** را به **مدیر سیستم، یا دیگر نقش‌ها** محدود نماید.	
۴٦	**مدیریت مشخصه های امنیتی ۳** - FMT_MSA.3.1
محصول باید مشخصه‌های امنیتی که برای اعمال **خط مشی** استفاده می‌شوند، باید مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.	
۴۷	**مدیریت مشخصه های امنیتی ۴** - FMT_MSA.3.2
محصول برای تعیین مقادیر اولیه پیشنهادی باید به **مدیر سیستم** اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد.	
۴۸	**مدیریت داده های محصول ۱-مدیر سیستم** - FMT_MTD.1.1(1)
محصول باید توانایی تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، **صفحات، اطلاعات و کاربران به مدیر سیستم یا دیگر نقش‌ها** محدود نماید.	
۴۹	**مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده** - FMT_MTD.1.1(2)
محصول باید توانایی تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن **داده‌های تحت مالکیت کاربر عادی** را به **کاربر عادی و مدیر سیستم** محدود نماید.	

۵۰	**کارکردهای مدیریتی محصول ۱** - FMT_SMF.1.1

محصول باید قادر به انجام **کارکردهای مدیریتی** که در جدول زیر آمده است باشد:

ردیف	مولفه استاندارد	مولفه	عملیات مدیریتي
۱	FAU_SAR.1	بازبيني داده مميزي ۱	• پشتيباني از (حذف، ويرايش، اضافه) گروهي از كاربران با مجوز دسترسي براي خواندن اطلاعات ركوردهاي مميزي
۲	FAU_SEL.1	انتخاب داده مميزي ۱	• پشتيباني از مجوزهاي مشاهده/ويرايش رويدادهاي مميزي
۳	FAU_STG.3	اقدامات لازم در زمان از دست رفتن داده مميزي	• پشتيباني از حدآستانه • پشتيباني از عمليات (حذف، ويرايش، اضافه) در زمان خرابي حتمي ذخيره سازي مميزي
٤	FAU_STG.4	ذخيره سازي رويدادهاي مميزي ۷	• پشتيباني از عمليات (حذف، ويرايش، اضافه) در زمان خرابي ذخيره سازي مميزي
٥	FDP_ACF.1	عمليات كنترل دسترسي ۱	• مديريت مشخصه هاي مورد استفاده براي ايجاد دسترسي و يا منع
٦	FDP_RIP.2	حفاظت از داده-هاي باقيمانده ۲	• انتخاب زمان اعمال حفاظت از اطلاعات باقي مانده (براي مثال به محض تخصيص يا حذف تخصيص) ميتواند توسط هدف ارزيابي قابل پيكربندي باشد.
۷	FDP_ITC.2	ورود داده هاي كاربري به محصول ٤	• ويرايش قوانين كنترلي بيشتر براي وارد كردن داده به داخل محصول
۸	FDP_SDI.2	صحت داده هاي كاربري ذخيره شده ۲	• عملياتي براي تشخيص يک خطاي صحت داده كه مي تواند قابل پيكربندي باشد.
۹	FIA_AFL.1	مديريت احراز هويت ناموفق ۱	• مديريت حدآستانه براي تلاش هاي ناموفق • مديريت عملياتي كه هنگام رويداد شكست

			احرازهویت باید صورت گیرد.
١٠	FIA_ATD.1	تعریف مشخصات کاربر ١	• مدیر مجاز باید قادر به تعریف مشخصه هاي امنیتي بیشتر براي کاربران باشد، اگر در الزامات مشخص شده باشد.
١١	FIA_SOS.1	مدیریت کلمه عبور	• مدیریت معیارها براي بررسي کلمه عبورها
١٢	FIA_UAU.1	زمانبندي احراز هویت	• مدیریت داده احرازهویت توسط مدیر • مدیریت داده احرازهویت توسط کاربر مرتبط • مدیریت لیست اقدامات قبل از اینکه کاربر احرازهویت شود
١٣	FIA_UAU.5	سازوکار احرازهویت چندگانه	• مدیریت مکانیزم هاي احرازهویت • مدیریت قوانین احرازهویت
١٤	FIA_UID.1	شناسایي کاربر	• مدیریت شناسه هاي کاربر • مدیریت لیست اقدامات اگر یک مدیر احرازشده بتواند اقدامات مجاز قبل از احرازهویت را تغییر دهد
١٥	FIA_USB.1	انقیاد مشخصه هاي امنیتي کاربر با موجودیت فعال متناظر١	• مدیر مجاز میتواند مشخصه هاي امنیتي موجودیت هاي فعال پیش فرض را تعریف کند. • مدیر مجاز میتواند مشخصه هاي امنیتي موجودیت هاي فعال را تغییر دهد.
١٦	FMT_MOF.1	مدیریت رفتار توابع امنیتي	• مدیریت گروهي از نقش هایي که با توابع امنیتي هدف ارزیابي در تعامل هستند.
١٧	FMT_MSA.1	مدیریت مشخصه هاي امنیتي ١	• مدیریت گروهي از نقش هایي که با مشخصه هاي امنیتي در تعامل هستند. • مدیریت نقش هایي که مشخصه هاي امنیتي مقادیر معیني را به ارث میبرند.

۱۸	FMT_MSA.3	مدیریت مشخصه هاي امنیتي ۳	• مدیریت گروهي از نقش هایي که مقادیر اولیه را مشخص میکنند. • مدیریت تنظیمات محدودکننده و مجازکننده مقادیر پیش فرض براي سیاست هاي کنترل دسترسي • مدیریت قوانیني که مشخصه هاي امنیتي مقادیر معیني را به ارث میبرند.
۱۹	FMT_MTD.1(1)	مدیریت داده هاي محصول ۱-مدیر سیستم	• مدیریت گروهي از قوانیني مرتبط با داده هاي توابع امنیتي هدف ارزیابي
۲۰	FMT_MTD.1(2)	مدیریت داده هاي محصول ۱- کاربرعادي، وارد کننده داده	• مدیریت گروهي از قوانیني مرتبط با داده هاي توابع امنیتي هدف ارزیابي
۲۱	FMT_SMR.1	نقش هاي امنیتي ۱	• مدیریت گروهي از کاربراني که بخشي از یک نقش هستند.
۲۲	FTA_MCS.1	محدودیت بر روي چندین نشست همزمان ۱	• مدیریت حداکثر تعداد مجاز نشست هاي همزمان کاربران توسط مدیر
۲۳	FTA_TSE.1	برقراري نشست ۱	• مدیریت شرایط برقراري نشست توسط مدیر مجاز
۲٤	FTA_SSL.3	قفل گذاري بر روي نشست‌ها و خاتمه دان به آنها	• تعیین زمان غیرفعال بودن کاربر پس از آنکه پایان نشست براي هر کاربر روي داده است • تعیین زمان پیش فرض غیرفعال بودن کاربر بعد از پایان نشست هاي تعاملي

۵۱	**نقش های امنیتی ۱** - FMT_SMR.1.1
نقش‌هاي زير در محصول بايد تعريف شده باشد: **مدیر سیستم،** **کاربر عادی،** **اپراتور ورود اطلاعات،** **مهمان**	
۵۲	**نقش‌های امنیتی ۲** - FMT_SMR.1.2
محصول، بايد قادر به مرتبط نمودن كاربران با نقش‌هاي مجاز تعريف شده باشند.	

۵,٦ کلاس حفاظت از محصول

شماره الزام	عنصر امنیتی
۵۳	**حفظ وضعیت امن در زمان شکست ۱** - FPT_FLS.1.1
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: **شکست‌های نرم‌افزاری، شکست‌های سخت افزاری**	
۵۴	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۱** - FPT_TDC.1.1
محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار **دادهای احراز هویت** را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد.	
۵۵	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۲** - FPT_TDC.1.2
محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، **چک کردن Hash اطلاعات دریافتی از آنها** استفاده نماید.	
۵٦	**انتقال داده امنیتی در داخل محصول ۱** - FPT_ITT.1.1
محصول باید هنگام انتقال داده‌ها بین بخش‌های مجزای خود، در برابر افشاء یا تغییر محافظت نماید.	
۵۷	**مهرهای زمانی ۱** - FPT_STM.1.1
محصول، بايد قادر به ايجاد مهره‌هاي زماني قابل اطمينان باشند و یا این نیازمندی را از طریق سرورهای امن و مکانیزم کارکردی صحیح برطرف نماید.	

۵۸	**به روز رسانی امن ۲** - FPT_TUD_EXT.1.2
محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی فراهم کندکه به‌روزرسانی نرم‌افزار و میان‌افزارمیان‌افزار محصول مورد ارزیابی را به صورت دستی آغاز نماید و از هیچ مکانیسم به‌روزرسانی دیگری پشتیبانی نکند. *نرم افزار پورتال امکان به روز رسانی خودکار ندارد لذا این ایتم برای محصول کارکرد ندارد. بروز رسانی به صورت دستی و توسط کارشناسان شرکت انجام می شود.*	

۵,۷ کلاس دسترسی به محصول

شماره الزام	عنصر امنیتی
۵۹	**محدودیت بر روی چندین نشست همزمان ۱** - FTA_MCS.1.1
محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	
٦٠	**محدودیت بر روی چندین نشست همزمان ۲** - FTA_MCS.1.2
محصول باید به صورت پیش‌فرض، **تعداد نشست همزمان پیش‌فرض که قابل تنظیم است را** برای هر کاربر در نظر بگیرد.	
٦١	**قفل کردن و خاتمه دادن به نشست ها ۵** - FTA_SSL.3.1
محصول باید کلیه نشست‌های تعاملي راه دور[3] را پس از مدت زمان **بازه زمانی که توسط مدیرتنظیم می‌شود** غیرفعال بودن، خاتمه دهد.	
٦٢	**قفل کردن و خاتمه دادن به نشست ها ٦** - FTA_SSL.4.1
محصول باید اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.	
٦٣	**سوابق دسترسی به محصول ۱** - FTA_TAH.1.1
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش (موفق / ناموفق) برای ایجاد نشست براساس روز، زمان، **آدرس IP** باشد.	

[3]Remote

٦۴	**سوابق دسترسی به محصول ۲** - FTA_TAH.1.2
در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید روز، زمان، مکان آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.	
٦۵	**سوابق دسترسی به محصول ۳** - FTA_TAH.1.3
محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک نماید.	
٦٦	**برقراری نشست ۱** - FTA_TSE.1.1
توابع امنیتي هدف ارزیابي باید بتواند از برقراري نشست براساس تعداد تلاش هاي ناموفق احرازهویت، شناسه کاربر، محدوده IP ممانعت نماید.	

۵،۸ کلاس کانال‌ها/مسیرهای مورد اعتماد

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

شماره الزام	عنصر امنیتی
٦٧	**کانال امن ۱** - FTP_ITC.1.1
محصول می تواند مسیر ارتباطي امنی را با استفاده از پروتکل HTTPS و TLS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی، سرور احرازهویت (Active Directory) ، **سرور پست الکترونیک، سرور پایگاه داده** که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده‌هاي تبادلي در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
٦٨	**کانال امن ۲** - FTP_ITC.1.2
محصول مورد ارزیابی می تواند اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
٦٩	**کانال امن ۳** - FTP_ITC.1.3
محصول مورد ارزیابی می تواند ارتباطات را از طریق کانال امن، برای **ارسال اطلاعات هویتی** راه‌اندازی نماید.	
۷۰	**مسیر امن ۱** - FTP_TRP.1.1
محصول باید قادر باشد در صورت فراهم بودن زیر ساخت لازم با استفاده از پروتکل TLS میسر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه دور ایجاد شود که به طور منطقی از دیگر کانال ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء دادهای تبادلی حفاظت نماید و تغییرات را تشخیص دهد.	

۷۱	**مسیر امن ۲ -** FTP_TRP.1.2
محصول مورد ارزیابی می تواند به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۷۲	**مسیر امن ۳ -** FTP_TRP.1.3
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 کلاس تخصیص منابع

شماره الزام	عنصر امنیتی
۷۳	**تحمل خطا ۱ -** FRU_FLT.1.1
توابع امنيتي هدف ارزيابي بايد نسبت به عملكرد **تمام كاركردهاي اصلي هدف ارزيابي** در زمان رخ دادن شكست‌هاي زير اطمينان حاصل نمايد: شكست نرم‌افزاري	

۵,۱۰ توجیهات

۷۴	**تولید کلید رمز نگاری ۱ -** FCS_CKM.1.1
محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم های 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. *با توجه به اینکه در محصول جهت نگهداری رمزعبور کاربران و بررسی صحت داده ممیزی از عملیات Hash استفاده می شود، الزامات مربوط به از بین بردن کلید و تولید کلید در محصول کاربرد ندارد.* *نرم افزار پورتال رمزنگاری نامتقارن را با استفاده از وب سرور انجام می دهد لذا خود پورتال کارکرد تولید کلید رمزنگاری نامتقارن را ندارد.*	

۷۵	**مدیریت کلید رمزنگاری ۱** - FCS_CKM_EXT.4.1

محصول باید براساس متد تخریب کلید **رمزنگاری رونویسی با صفر** که بر اساس استاندارد **زیر** باشد، کلیدهای رمزنگاری را از بین ببرد.

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.

با توجه به اینکه در محصول جهت نگهداری رمزعبور کاربران و بررسی صحت داده ممیزی از عملیات Hash استفاده می شود، الزامات مربوط به از بین بردن کلید و تولید کلید در محصول کاربرد ندارد.

نرم افزار پورتال رمزنگاری نامتقارن را با استفاده از وب سرور انجام می دهد لذا خود پورتال کارکرد تولید کلید رمزنگاری نامتقارن و تخریب کلید رمزنگاری را ندارد.

۷٦	**الزامات پروتکلTLS Server/ احراز هویت ۱** - FCS_TLSS_EXT.1.1

محصول باید 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**
  - LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268

الزامات TLSS توسط محیط عملیاتی پوشش داده شده‌اند و الزامات این مؤلفه توسط هدف ارزیابی پیاده‌سازی نشده‌است

۷۷	**الزامات پروتکلTLS Server/ احراز هویت ۲** - FCS_TLSS_EXT.1.2

محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1، هیچ‌کدام دارند، رد نماید.

الزامات TLSS توسط محیط عملیاتی پوشش داده شده‌اند و الزامات این مؤلفه توسط هدف ارزیابی پیاده‌سازی نشده‌است

۷۸	**الزامات پروتکلTLS Server/ احراز هویت ۳** - FCS_TLSS_EXT.1.3
محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت ایجاد نماید. *الزامات TLSS توسط محیط عملیاتی پوشش داده شده‌اند و الزامات این مؤلفه توسط هدف ارزیابی پیاده‌سازی نشده‌است*	
۷۹	**ورود داده های کاربری به محصول ۴** - FDP_ITC.2.1
محصول باید هنگام دریافت داده کاربری، **خط‌مشی کنترل دسترسی** را اعمال نماید. *با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.*	
۸۰	**ورود داده های کاربری به محصول ۵** - FDP_ITC.2.2
محصول باید از مشخصه‌های امنیتی مرتبط با داده‌های کاربری را هنگام ورود داده‌ها استفاده نماید. *با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.*	
۸۱	**ورود داده های کاربری به محصول ٦** - FDP_ITC.2.3
محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال، ارتباط و همبستگی بین مشخصه‌های امنیتی و داده کاربری دریافت شده را فراهم می‌نماید. *با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.*	

۸۲	**ورود داده های کاربری به محصول ۷** - FDP_ITC.2.4
محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، می‌باشد. *با توجه به آنکه امضاي ديجيتال داده‌هاي كاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط كاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امكان ارزيابي اين الزام وجود ندارد.*	
۸۳	**ورود داده های کاربری به محصول ۸** - FDP_ITC.2.5
توابع امنيتي هدف ارزيابي بايد در هنگام ورود داده كاربري تحت كنترل خط‌مشي- امنيتي از خارج هدف ارزيابي، قوانين زير را اعمال نمايد: *[الزام: در هنگام ورود ركوردهاي الكترونيكي، هدف ارزيابي بايد صحت ركوردها را از بررسی Hash مربوط به ركوردها بررسي نمايد.]* *با توجه به آنکه امضاي ديجيتال داده‌هاي كاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط كاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امكان ارزيابي اين الزام وجود ندارد.*	
۸۴	**خروج داده های کاربری از محصول ۳** - FDP_ETC.2.1
محصول باید هنگام خروج داده کاربری به بیرون **خط مشی کنترل دسترسی** را اعمال نماید *با توجه به آنکه امضاي ديجيتال داده‌هاي كاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط كاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امكان ارزيابي اين الزام وجود ندارد.*	
۸۵	**خروج داده های کاربری از محصول ۴** - FDP_ETC.2.2
محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون محصول)، مشخصه های امنیتی مرتبط با داده کاربری را نیز انتقال دهد.	

با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.	
٨٦	**خروج داده های کاربری از محصول ۵** - FDP_ETC.2.3
محصول باید اطمینان دهد که مشخصه های امنیتی در هنگام خروج داده از محصول، ارتباط پیوند شفافی با داده کاربری خارج شده دارند. *با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.*	
٨٧	**خروج داده های کاربری از محصول ٦** - FDP_ETC.2.4
محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال نماید: **مدیر سیستم باید خروج رکوردها را محدود نماید، به طوری‌که کاربران محصول بدون هدف قادر به خروج داده به بیرون از آن (خارج از محصول) نباشند.** *با توجه به آنکه امضاي ديجيتال داده‌هاي کاربري در هنگام ورود داده در سامانه‌هاي تحت وب مي‌تواند به عنوان مشخصه‌هاي امنيتي آن داده‌ها به شمار رود و در اين سامانه براي ورود داده‌ها توسط کاربران از امضاي ديجيتال بهره گرفته نمي‌شود، امکان ارزيابي اين الزام وجود ندارد.*	
٨٨	**مهرهای زمانی ۱** - FPT_STM.1.1
محصول، باید قادر به ایجاد مهره‌هاي زماني قابل اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و مکانیزم کارکردی صحیح برطرف نماید. *با توجه به اینکه نرم افزار پورتال مبتی بر وب می باشد مهرهای زمانی توسط سرور تولید می شود نه نرم افزار*	

۸۹	**به روز رسانی امن ۳-** FPT_TUD_EXT.1.3

محصول مورد ارزیابی باید 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.

نرم افزار پورتال امکان به روز رسانی خودکار ندارد لذا این ایتم برای محصول کارکرد ندارد. به روز رسانی به صورت دستی و توسط کارشناسان شرکت انجام می شود.

۵,۱۱ وابستگی های نیازمندی های کاربردی امنیتی

مؤلفه	وابستگي ها
FAU_GEN.1	- FPT_STM.1
FAU_GEN.2	- FAU_GEN.1 - FIA_UID.1
FAU_SAR.1	- FAU_GEN.1
FAU_SAR.2	- FAU_SAR.1
FAU_SAR.3	- FAU_SAR.1
FAU_SEL.1	- FAU_GEN.1 - FMT_MTD.1
FAU_STG.1	- FAU_GEN.1
FA_STG.3	- FAU_STG.1
FAU.STG.4	- FAU_STG.1
FCS_COP.1(1)	- [FDP_ITC.1 or - FDP_ITC.2 or - FCS_CKM.1] - FCS_CKM.4
FCS_COP.1(2)	- [FDP_ITC.1 or - FDP_ITC.2 or - FCS_CKM.1] - FCS_CKM.4

مؤلفه	وابستگي ها
FDP_ACC.1	- FDP_ACF.1
FDP_ACF.1	- FDP_ACC.1 - FMT_MSA.3
FDP_RIP.2	-
FDP_ITC.2	- FDP_ACC.1 - [FTP_ITC.1 or - FTP_TRP.1] - FPT_TDC.1
FDP_ETC.2	- FDP_ACC.1
FDP_SDI.2	-
FIA_AFL.1	- FIA_UAU.1
FIA_ATD.1	-
FIA_SOS.1	-
FIA_UAU.1	- FIA_UID.1
FIA_UAU.5	-
FIA_UID.1	-
FIA_USB.1	- FIA_ATD.1
FMT_MOF.1	- FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1	- [FDP_ACC.1 or - FDP_IFC.1] - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.3	- FMT_MSA.1 - FMT_SMR.1
FMT_MTD.1(1)	- FMT_SMR.1 - FMT_SMF.1
FMT_MTD.1(2)	- FMT_SMR.1 - FMT_SMF.1
FMT_SMF.1	-

مؤلفه	وابستگي ها
FMT_SMR.1	- FIA_UID.1
FPT_FLS.1	-
FPT_TDC.1	-
FRU_FLT.1	- FPT_FLS.1
FTA_MCS.1	- FIA_UID.1
FTA_SSL.3	-
FTA_SSL.4	-
FTA_TAH.1	-
FTA_TSE.1	-

٦ الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است که بر اساس پروفایل حفاظتی می باشد.

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 هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۷ خلاصه مشخصات هدف ارزیابی

نسخه ۱,٦ سند هدف امنیتی پورتال تتیس توسط کمیته توسعه شرکت آرمان دنیای فناوری اطلاعات تتیس تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

- کلاس ممیزی امنیت

- محصول می تواند برای تمام رویدادهای ورود و خروج کاربر به/ از سیستم، کنترل دسترسی، مشخصه‌های امنیتی و دیگر رویدادهای قابل ممیزی رکورد ممیزی تولید نماید و برای هر رکورد ممیزی، حداقل اطلاعات IP ، نوع کاربری ، تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد کاربر، محل خدمت کاربر زیر را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند. (FAU_GEN.1.1, FAU_GEN1.2, FAU_GEN2.1)
- محصول دارای قابلیت خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش، حذف و ایجاد آیتم جدید، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم و کاربران مجاز و دارای قابلیت نمایش رکوردهای ممیزی را به شکل خوانا و قابل درك 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) و آدرس IP مرتب نماید. (FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR2.1, FAU_SAR.3.1)
- از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد. و محصول قادر به تشخیص تغییرات غیر مجاز در رکوردهای ممیزی می باشد و در صورت تجاوز دنباله ممیزی از مقدار مشخص شده برای مدیر سیستم یک ایمیل ارسال می کند (آدرس ایمیل مدیر سیستم در فایل web.config موجود در ریشه نرم افزار است در بخش configuration > appSettings > WebmasterEmail قابل تنظیم است) و در این حالت تعدادی از رویدادهای ممیزی قدیمی که توسط مدیر سیستم قابل تنظیم است از سیستم حذف می شود. (FAU_STG_1.1, FAU_STG.1.2, FAU_STG.3.1, FAU_STG.4.1)

- می توان در بخش تنظیمات، تنظیمات پورتال انواع رویدادها جهت ممیزی نمودن انتخاب نمود. (FAU_SEL.1.1)

- **کلاس پشتیبانی از رمزنگاری**

- محصول می تواند با استفاده از تنظیمات سیستم عامل و وب سرور مانند IIS از TLS 1.2 با Cypher Suite های مورد قبول نظیر TLS_RSA_WITH_AES_128_CBC_SHA پشتیبانی کند و اتصال کاربر با SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 را رد نماید. (FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.1.2, FCS_TLSC._EXT.1.3)
- محصول می تواند برای تولید داده درهم سازی به منظور صحت اطلاعات کاربر از الگورتیم SHA256 استفاده کند. به این نحوه که از اطلاعات رکورد یک متن XML ایجاد می نماید و سپس آن را با استفاده از الگوریتم SHA256 درهم سازی کرده و مقدار را در پایگاه داده ذخیره می کند. در هنگام بازیابی رکورد اطلاعاتی مجدد رکورد خوانده شده را مطابق فرآیند ذکر شده درهم سازی می نماید و با مقدار Hash ذخیره شده در پایگاه داده مقایسه می کند. در صورت عدم مطابقت پیام خطا می دهد. (FCS_COP1.1(1), FCS_COP.1.1(2))
- محصول گذرواژه کاربران را با استفاده از الگوریتم Bcrypt درهم سازی کرده و در پایگاه داده ذخیره می‌کند.

- **کلاس شناسایی و احرازهویت**

- رمز عبور سیستم می تواند ترکیبی از حروف کوچک و بزرگ و اعداد و برخی کاراکترهای خاص باشد و حداقل طول رمز عبور توسط مدیر سیستم در بخش تنظیمات پورتال قابل تعریف است. در بخش تنظیمات پورتال گزینه «پیچیدگی گذرواژه» قابل تنظیم است (FIA_PMG_EXT.1.1)
- 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. و در صورت تلاش بیشتر حساب کاربری را قفل کند این تنظیم از بخش تنظیمات پورتال گزینه «امکان قفل کردن کاربر»، «تعداد مجاز سعی گذرواژه غلط» قابل پیکربندی است. (FIA_AFL.1.1, FIA_AFL.1.2)

- محصول می تواند با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را در بخش تنظیمات پورتال مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد. این تنظیم از بخش تنظیمات پورتال گزینه «امکان قفل کردن کاربر»، «تعداد مجاز سعی گذرواژه غلط» قابل پیکربندی است. (FIA_AFL.1.1)
- محصول مشخصه های 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 بر ای هر کاربر نگهداری می نماید. (FIA_ATD.1.1)
- محصول پیش از شناسایی کاربر اجازه مشاوره و راهنمایی نحوه ورود به سیستم را می دهد و پیش از آنکه کاربر اقدامات میانی دیگری انجام دهد او را با موفقیت شناسایی می کند. از طریق راهنمایی در صفحه لاگین نرم افزار پورتال (FIA_UID.1.1, FIA_UID.1.2, FIA_UAU.1.1, FIA_UAU.1.2)
- محصول اقدامات زیر را برای احراز هویت مدیر سیستم می کند: نام کاربری و کلمه عبور، احراز هویت دو مرحله ای (ارسال ایمیل) و محصول هر کاربر متقاضی احراز هویت از راه دور علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه که تعریف شده استفاده می کند، پس از ورود نام کاربری و کلمه عبور یک کد امنیتی برای آنها ایمیل می شود و کد امنیتی را باید جهت تایید هویت در سیستم وارد نماید تا احراز هویت شود. امکان تعیین احراز هویت دو مرحله ای برای هر کاربر به صورت جداگانه از طریق بخش مدیریت کاربران پورتال قابل تنظیم است (FIA_UAU5.1, FIA_UAU.5.2)
- محصول می تواند مشخصه های امنیتی شناسه کاربر، نقش های کاربر، مجموعه دسترسی های کاربر به بخش های مختلف، جزییات واسط کلاینت (مرورگر، IP)، پیشینه احراز هویت (زمان، آخرین تلاش احراز هویت 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.
- و در صورت اتصال کاربر در نشست جدید نشست اول را از آن مطلع می نماید. هنگام ورود آخرین لاگ‌های ورود موفق به سیستم را نمایش می دهد (FIA_USB.1.1, FIA_USB.1.2)
    - 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 هیچ تغییری در طول تشست فعال را مجاز نمی داند (FIA_USB.1.3)
- محصول می تواند گواهی نامه ها را جهت ارتباط با سرور ایمیل و سرور Active Directory بررسی نماید و باید شامل موارد زیر باشند و مدیر سیستم می تواند در بخش تنظیمات پورتال با استفاده از گزینه های بررسی فیلدهای اضافه گواهی و گزینه اعتبارسنجی زنجیره و لیست Rev گواهی ها اعتبارسنجی و یا عدم اعتبارسنجی گواهی نامه ها را تعیین نماید. (FIA_X509_EXT.1.1/Rev, FIA_X509_EXT.1.2/Rev, FIA_X509_EXT.2.1, FIA_X509_EXT.2.2):
  - حداقل طول ۳ در زنجیره گواهی نامه شامل ریشه خود امضا، گواهی واسط و گواهی نامه هویت سرور
  - یکی از گواهی های مسیر دارای پرچم CA برابر True بوده و دارای افزونه Basic Constraints باشد
  - گواهی نامه سرور ایمیل یا Active Directroy باید هدف Server Authentication در فیلد extendedKeyUsage را داشته باشد
  - بررسی وضعیت فسخ گواهی نامه ها از طریق CRL هنگام ارسال ایمیل به سرور ایمیل و یا هنگام احراز هویت کاربر توسط Active Directroy انجام می پذیرد

- کلاس حفاظت از داده کاربری

- محصول تضمین می کند که هر گونه محتوی اطلاعات قبلی یک منبع را هنگام تخصیص منابع به تمام موجودیت های غیرفعال استفاده شده، غیر قابل دسترسی کند. (FDP_RIP.2.1)
- محصول هنگام دریافت داده کاربری خط مشی کنترل دسترسی را اعمال می کند و صحت داده ها را با بررسی Hash مربوطه بررسی می نماید. (FDP_SDL.2.1, FDP_ACF.1.1, FDP_ACF.1.2)
- محصول داده های کاربری ذخیره شده در مکان تحت کنترل خود را برای خطاهای صحت داده رکورد و داده های ممیزی را بر اساس مشخصه های درهم شده داده های کاربری ذخیره شده پایش نماید و هنگام تشخیص خطای صحت داده، باید از نمایش رکورد جلوگیری کند. به این صورت که از اطلاعات یک متن XML ایجاد می شود و این متن XML با استفاده از الگورتیم SHA256 درهم ریزی می شود و مقدار درهم شده در پایگاه داده ذخیره می شود در هنگام خواندن رکورد برای اطلاعات خوانده شده

مجددا عبارت درهم شده ایجاد می شود و مقدار محاسبه شده با مقدار ذخیره شده در پایگاه داده مقایسه می شود در صورتیکه این دو عبارت یکسان بودند به این معنی است که رکورد توسط پورتال ویرایش شده است و در صورتیکه این دو عبارت متفاوت بود به این معنی است که رکورد خارج از پورتال تغییر کرده است و کاربر پیام خطای مناسب را در این حالت دریافت می کند (DP_SDI.2.1, DP_SDI.2.2)

- محصول باید خط مشی های کنترل دسترسی را بر روی موجودیت فعال و موجودیت غیرفعال و عملیات اعمال نماید. نحوه اعمال دسترسی بر رکورد موجودیت های فعال و غیر فعال به این صورت است که مدیری سیستم می توان از بین مجوزهای تعریف شده برای هر موجودیت دسترسی مربوطه را به یک گروه و یا یک کاربر اعطا نماید. همچنین امکان تعریف دسترسی در سطح کل مثلا اطلاعات پورتال و تعاریف فرا داده های آن نظیر صفحات و دسته بندی ها وجود دارد و با اعمال دسترسی در آن سطح کاربران حق دسترسی به تمامی رکوردهای موجود در آن بخش را خواهند داشت. با توجه به تعدد رکوردها و بخش های اطلاعات و با توجه به امکان تعریف سطح دسترسی مجزا حتی برای یک رکورد امکان ایجاد محیطی که تمام دسترسی های کاربر در آن قابل مشاهده باشد عملی نیست و این امکان از طریق گزینه مربوطه در هر موجودیت فعال و غیر فعال ممکن می باشد. (FDP_ACC.1.1)
- محصول خط مشی های کنترل 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 را بر روی موجودیتی های غیرفعال اعمال می نماید و 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. (FDP_ACF.1.1, FDP_ACF.1.2)
- محصول می تواند با استفاده از 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 احزار هویت، به اطلاعات قابل دسترس عموم دسترسی دارند. (رکوردهای منتشره شده – Published – از جمله فایلها، اگر فایلی منتشر شده باشد کاربران بدون نیاز به احراز هویت دسترسی مشاهده فایل ها منتشر شده را خواهند داشت) (FDP_ACF.1.3)

- محصول صرحتا بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: تعداد درخواست های بالای ناگهانی از یک یا بیشتر از یک IP مشخص، تجاوز تعداد تلاش های احراز هویت یک کاربر مشخص از مقدار آستانه از پیش تعریف شده، تعداد درخواست های بالای ناگهانی از یک کاربر مجاز، تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده. (FDP_ACF.1.4)

- **کلاس مدیریت امنیت**

- محصول تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار کارکرد تمام کارکردهای مربوط به مدیریت محصول را به مدیر سیستم یا دیگر نقشها محدود نماید. محصول با اعمال خطمشی کنترل دسترسی، توانايي تغيير پيشفرض، پرس و جو، تغییر، حذف مشخصه هاي امنيتي و مجوزهایی که کاربران بر روی اطلاعات وجود دارد سیستم داده می شود را به مدیر سیستم، یا دیگر نقشها محدود می‌نماید. محصول مشخصه هاي امنيتي که براي اعمال خط مشی استفاده میشوند، باید مقادیر پیش فرض محصول براي تعيين مقادير اوليه پيشنهادي بايد به مدير سيستم اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد. محصول براي تعيين مقادير اوليه پيشنهادي به مدير سيستم اجازه می دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد. (FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2)
- محصول تغییر پیشفرض، پرسوجو، تغییر، حذف، پاك نمودن صفحات و اطلاعات و کاربران را به مدیر سیستم یا دیگر نقشها محدود می نماید. محصول امکان تغییر پیشفرض، پرسوجو، تغییر، حذف، پاك نمودن داده های تحت مالکیت کاربر عادی را به کاربر عادی و مدیر سیستم محدود می کند (FMT_MTD.1.1(1), FMT_MTD.1.1(2))
- محصول توانایی انجام کارکردهای مدیریتی را دارد (FMT_SMF.1.1)
  - مدیر سیستم می تواند دسترسی مشاهده اطلاعات رویدادنگاری را به یک یا گروهی از کاربران داده و یا از آنها بگیرد (FAU_SAR.1) هنگامی که کاربر وارد بخش رویدادها > لاگ عملکرد کاربر شود و یا روی دکمه مشاهده یکی از رکوردهای لاگ موجود کلیک کند در صورتیکه این

تنظیم فعال باشد سابقه این مشاهده در رویدادنگاری به صورت زیر ثبت می شود. (عمل: View ، نوع AuditLogEntry)

- مدیر سیستم می توان در بخش تنظیمات بخش تنظیمات پورتال انواع رویدادها جهت ممیزی شدن را انتخاب نموده و یا از انتخاب خارج نماید (FAU_SEL.1)
- مدیر سیستم می تواند حد آستانه تعداد رکوردهای ممیزی را در بخش تنظیمات مشخص نماید (FAU_STG.3)
- مدیر سیستم تعیین می کند که در زمان رسیدن تعداد رکوردها به حد آستانه چه تعداد رکورد قدیمی حذف شده و مجدد روی آنها رونویسی انجام شود (FAU_STG.4)
- در زمان خرابی رویدادنگاری رکوردهای رویدادنگاری برای مدیر سیستم ایمیل می شود (ایمیل مدیر سیستم از طریق فایل web.config بخش WebmasterEmail قابل تنظیم است) (FAU_STG.4)
- مدیر سیستم می تواند دسترسی هر یک از موجودیت های فعال را به هر یک از موجودیت های غیر فعال تعیین نماید که شامل دسترسی و یا منع می شود (FDP_ACF.1)
- مدیر سیستم می تواند زمان انقضای نشست را از بخش تنظیمات پورتال مشخص نماید که پس از آن زمان اطلاعات نشست کاربر جاری از سرور حذف می گردد (FDP_RIP.2)
- مدیر سیستم می تواند مشخص نماید میزان محدود بودن کاربران جهت ثبت ورود اطلاعات به سیستم چه میزان باشد به عنوان مثال منع از ورود اسکریپت در اطلاعات و یا عدم بارگزاری فایل های خطرناک. این تنظیمات در بخش تنظیمات پورتال قابل پیکربندی می باشند. (FDP_ITC.2)
- مدیر سیستم می تواند تعیین کند که برای رکوردهای اطلاعات Hash صحت رکورد بررسی شود یا خیر (FDP_SDI.2)
- مدیر سیستم می تواند تعیین کند که حساب کاربری کاربر پس از چند بار احراز هویت ناموفق قفل شود. از طریق بخش تنظیمات پورتال (FIA_AFL.1)

- مدیر سیستم می تواند یک کاربر را غیر فعال نماید و همچینن آدرس ایمیل کاربر را تعریف نماید و تعیین کند که کاربر احراز هویت دومرحله ای داشته باشد. از طریق بخش مدیریت کاربران (FIA_ATD.1)
- مدیر سیستم می تواند تعیین کند که کاربران مجبور به انتخاب گذرواژه پیچیده باشند. از طریق بخش تنظیمات پورتال (FIA_SOS.1)
- مدیر سیستم می تواند تعیین کند که کاربران از یک سری آدرس های IP مشخص شده و در یک بازه های زمانی مشخص شده امکان احراز هویت نداشته باشند. از طریق بخش تنظیمات پورتال (FIA_UAU.1)
- مدیر سیستم می تواند تعیین کند که کدام کاربران باید احراز هویت دو مرحله ای داشته باشند. از بخش مدیریت کاربران (FIA_UAU.5)
- مدیر سیستم می تواند کاربران سیستم را تعریف نموده و آنها را فعال و غیر فعال نماید و مشخص نماید از کدام ادرسهای IP و در کدام زمان ها امکان ورود به سیستم را داشته باشند. از بخش مدیریت کاربران و بخش تنظیمات پورتال (FIA_UID.1)
- مدیر سیستم می تواند دسترسی هایی برای گروه های سیستم تعریف نماید که در هنگام ایجاد کاربر جدید در سیستم با توجه به حوزه فعالیت کاربر آن کاربر عضو یکی از این گروه ها شود همچنین مدیر سیستم تواند سطح دسترسی کاربران فعلی را نیز تغییر داده و ویرایش نماید (FIA_USB.1, FMT_MSA.3)
- مدیر سیستم می تواند گروه ها و نقش های سیستم را تعریف نموده و دسترسی گروه ها و نقش های سیستم را تعیین نماید (FMT_MOF.1, FMT_MSA.1)
- مدیر سیستم می تواند دسترسی کاربران مدیر و کاربران عادی را جهت دسترسی داشتن مشاهده و ویرایش اطلاعات تعیین نماید ((FMT_MTD.1(1), FMT_MTD.1(2)
- مدیر سیستم می تواند عضویت کاربران در گروه ها و نقش ها را تعیین نماید (FMT_SMR.1)
- مدیر سیستم می تواند تعیین کند که یک کاربر امکان ورود به سیستم را از طریق چند نشست همزمان نداشته باشد. در بخش مدیریت کاربران قابل انجام است (FTA_MCS.1)

- مدیر سیستم می تواند تعیین کند که کاربر از چه آدرس های IP و در چه زمان هایی امکان ایجاد نشست جدید را دارد. از بخش تنظیمات پورتال قابل تنظیم است (FTA_TSE.1)
- مدیر سیستم می تواند تعیین کند میزان زمان غیر فعال بودن کاربر جهت خاتمه نشست چه مقدار باشد. از بخش تنظیمات پورتال قابل تنظیم است. (FTA_SSL.3) این تنظیم باید صرفا از بخش تنظیمات پورتال انجام پذیرد و برای نشست هایی که بعد از تغییر این مقدار آغاز می شنود اعمال خواهد شد.

- نقش های زیر در محصول تعریف شده است: مدیر سیستم، کاربر عادی، اپراتور ورود اطلاعات، مهمان و محصول قادر به مرتبط نمودن کاربران با نقش های مجاز تعریف شده است. (FMT_SMR.1.1, FMT_SMR1.2)
- 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 پیش فرض را لغو و تغییر دهد.
- محصول می تواند توانایی تغییر پیشفرض، پرس و جو، تغییر، حذف، پاك 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.
- در محصول می توان در هر یک از ماژول های سیستم نقش‌های 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.

- **کلاس حفاظت از محصول**

- 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 باید در زمان رخداد انواع شکستهاي زیر، وضعیت امن را حفظ نمایند: شکستهای نرم افزاری، شکستهای سخت افزاری (FPT_FLS.1.1)
- با توجه به اینکه محصول پورتال است و به صورت کاملا مبتنی بر وب می باشد لذا مهرهای زمانی تولید نکرده و از مهر های زمانی سرور استفاده می کند (FPT_STM.1.1)
- محصول در صورت استفاده از محصولات امن IT، تفسیر سازگار دادهای احراز هویت را در زمان اشتراك گذاري داده هاي امنيتي بين خود و ديگر محصولات امن IT، فراهم آورد. محصل باید هنگام تفسیر داده های دریافتی از دیگر محصولات IT امن، چک کردن اعتبار آن را از طریق فراخوانی وب سرویس‌های ارائه شده استفاده نماید. (FPT_TDC.1.1, FPT_TDC.1.2)
- محصول باید هنگام انتقال داده ها بین بخشهاي مجزاي خود، در برابر افشاء یا تغییر محافظت نماید. (FPT_ITT.1.1)
- محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می باشد که آنها را از سرور دریافت می کند (FPT_TUD_EXT.1.2)

- محصول مورد ارزيابي بايد اين امكان را براي مدير سيستم امنيتي فراهم كندكه به روز رساني نرم افزار و ميان افزار ميان افزار محصول مورد ارزيابي را به صورت دستي آغاز نمايد و از هيچ مكانيسم به روز رساني ديگري پشتيباني نكند. محصول مورد ارزيابي بايد در صورت استفاده از به روز رساني به روش خودكار، پيش از نصب به روزرساني هاي نرم افزاري و ميان افزاري، با استفاده از درهم ساز منتشرشده، ابزاري را براي احراز هويت ميان افزار آنها در اختيار محصول مورد ارزيابي قرار دهد. با توجه به اینکه محصول پورتال امکان بروز رسانی خودکار را ندارد، لذا این موارد در پورتال کاربرد ندارد. (FPT_TUD_EXT.1.2, FPT_TUD_EXT.1.3)

- **کلاس دسترسی به محصول**

- محصول بايد حداكثر تعداد نشستهاي همزمان متعلق به يک كاربر را محدود نمايد. می توان از بخش مدیریت کاربران این را تنظیم نمود.
- محصول بايد به صورت پيشفرض، تعداد نشست همزمان پيشفرض كه قابل تنظيم است را براي هر كاربر در نظر بگيرد. (FTA_MCS.1.1, FTA_MCS.1.2)
- محصول بايد كليه نشستهاي تعاملي راه دور را پس از مدت زمان بازه زمانی که توسط مدیر تنظیم می شود غیر فعال بود خاتمه دهد.
- محصول بايد اجازه خاتمه نشست، از سوي كاربري كه خود آغازگر نشست بوده است را بدهد. (FTA_SSL.3.1, FTA_SSL.4.1)
- در صورت برقراري نشست به طور موفقيت آميز، محصول بايد قادر به نمايش آخرين تلاش (موفق / ناموفق) برای ایجاد نشست بر اساس آدرس روز، زمان IP باشد. ، محصول بايد قادر به نمايش آخرين تلاش ناموفق براي ايجاد نشست براساس روز، زمان، آدرس IP و تعداد تلاش ناموفق تا آخرين ايجاد نشست موفقيت آميز باشد. محصول نبايد اطلاعات سوابق دسترسي را بدون بازديد كاربر از واسط كاربري پاك نمايد. (FTA_TAH.1.1, FTA_TAH.1.2, FTA_TAH.1.3)
- توابع امنيتي هدف ارزيابي بايد بتواند از برقراري نشست براساس تعداد تلاش هاي ناموفق احرازهويت، شناسه كاربر، محدوده IP ممانعت نمايد. (FTA_TSE.1.1)

- **کلاس کانال ها / مسیرهای مورد اعتماد**

- محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احراز هویت که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آنها را احراز هویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند اجازه داشته باشد به موجودیت های 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 دارند. (FTP_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3)

- **کلاس تخصیص منابع**

- توابع امنیتي هدف ارزیابي باید نسبت به عملکرد تمام کارکردهای اصلی محصول در زمان رخ دادن شکست نرم افزاری اطمینان حاصل نماید (FRU_FLT.1.1)