به نام خدا

سند هدف امنیتی

سامانه مدیریت و یکپارچه‌سازی داده‌های مکانی ژئوتاژک – نسخه ۳,۲,۲

شرکت دانش‌بنیان سامانه‌های آزاد فناوری اطلاعات ایده‌آل آینده ایرانیان - سافا

مرداد ماه ۱۴۰۲

نسخه ۱,۷

فهرست

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سامانه مدیریت و یکپارچه‌سازی داده‌های مکانی ژئوتاژک – نسخه ۳,۲,۲
نسخه	۱,۶
تاریخ	۱۴۰۲/۰۵/۱۰
نویسندگان	واحد تحقیق و توسعه شرکت دانش‌بنیان سافا

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت دانش‌بنیان سامانه‌های آزاد فناوری اطلاعات ایده‌آل آینده ایرانیان- سافا
نام محصول	سامانه مدیریت و یکپارچه‌سازی داده‌های مکانی ژئوتاژک
نوع محصول	برنامه کاربردی تحت وب
نسخه	۳,۲,۲

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

- ✓ **ممیزی امنیت:** محصول براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید می‌نماید:
  - آغاز و اتمام توابع ممیزی
  - تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده‌هایی که بار حقوقی دارند)
- ✓ **پشتیبانی از رمزنگاری:** محصول باید برای وارسی صحت داده‌های ممیزی و داده‌های رکورد بر اساس یک الگوریتم رمزنگاری مشخص و اندازه کلید رمزنگاری اجرا می‌شود که مطابق با استانداردهای موجود می‌باشد.
- ✓ **حفاظت از داده کاربری:** محصول خط‌مشی‌های کنترل دسترسی را بر روی موارد زیر اعمال می‌نماید:
  - موجودیت فعال: مدیر سیستم، کاربر عادی
  - موجودیت غیرفعال:
    - رکوردها، مستندات و فراداده

- داده متعلق به کاربران
- داده احرازهویت
- داده با این معیارها

- عملیات:
  - ایجاد موجودیت غیرفعال جدید
  - حذف موجودیت غیرفعال
  - تغییر دسترسی‌ها به موجودیت غیرفعال
  - عملیات بر روی فراداده وابسته به موجودیت غیرفعال

- ✓ **شناسایی و احرازهویت:** محصول می‌تواند با استفاده از یک عدد مثبت قابل تنظیم توسط مدیر در بازه قابل قبولی از مقادیر، تلاش‌های ناموفق احرازهویت مرتبط با لیستی از رویدادهای احرازهویت را تشخیص می‌دهد.
- ✓ **مدیریت امنیت:** محصول امکان تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار توابع تمام کارکردهای مربوط به مدیریت محصول را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود می‌نماید.
- ✓ **حفاظت از توابع امنیتی محصول:** محصول در زمان رخداد انواع شکست‌های نرم‌افزاری و سخت‌افزاری، وضعیت امن را حفظ می‌نمایند.
- ✓ **تخصیص منابع:** محصول از عملکرد تمام کارکردهای اصلی هنگام رویداد شکست‌های نرم‌افزاری و دیگر شکست‌ها اطمینان حاصل می‌نماید.
- ✓ **دسترسی به محصول:** محصول حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود می‌نماید.
- ✓ **کانال‌های/مسیرهای مورد اعتماد:** محصول قادر است در صورت فراهم بودن زیر ساخت لازم با استفاده از پروتکل TLS, HTTPS مسیر ارتباطی امنی فراهم می‌نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد.

۲-۳-۱- نوع هدف ارزیابی

سامانه مدیریت و یکپارچه سازی داده‌های مکانی ژئوتاژک مطابق با پروفایل برنامه کاربردی تحت شبکه، یک سامانه تحت وب می‌باشد.

۳-۳-۱- 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 Processeor X5690 (3.46 GHz, 6-core, 12Mb Cache, 130W, DDR3 – 1333)
فضای آزاد دیسک	60 GB
حافظه	8 GB or Higher
سیستم‌عامل	Linux Debian 10.9 64bit
DBMS	PostgreSQL
سایر نرم‌افزارها	Docker, NginX, MongoDB, RabbitMQ, Redis, Angular 9, GeoServer

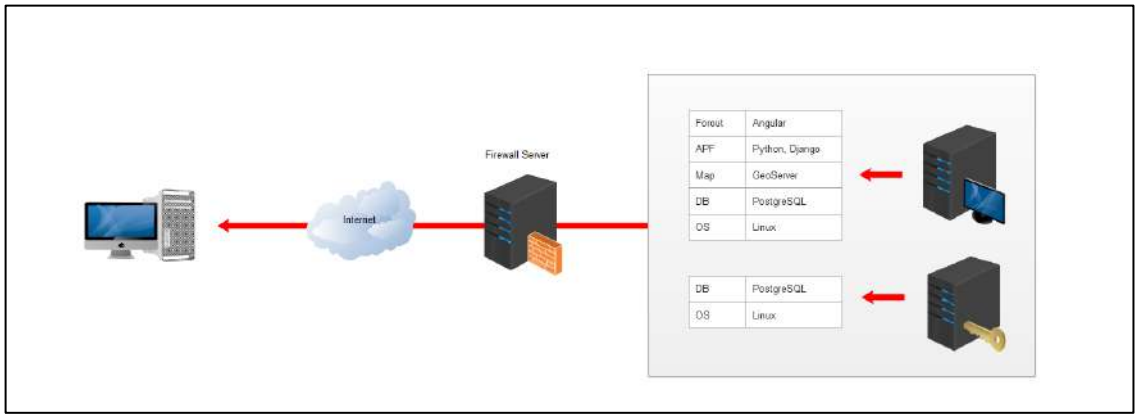
۴-۱- توصیف هدف ارزیابی

۱-۴-۱- حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
Linux	Debian 10.9 - 64bit &
PostgreSQL	11
Docker	20.10.06
Firewall	فایروال هر سازمان مختص به آن سازمان بوده و مستقل از نرم‌افزار GeoTajak می‌باشد

در این بخش قرارگیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شود. لازم است محصول و محیط عملیاتی به تفکیک در تصویر مشخص گردند.



۲-۴-۱- حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می شود که باید به صورت مشخص هریک از کارکردها و شرح آن‌ها در این قسمت مطرح شود.

کارکردها	توصیف
تنظیم ورود و خروج با استفاده از Password Complexity	تنظیمات آن در اختیار مدیر سیستم می‌باشد
رویدادنگاری با استفاده MongoDB	مشاهده تمامی فعالیت‌های انجام شده توسط کاربران
لاگین به نرم‌افزار با استفاده از Django	شناسایی هویت فرد با استفاده از فریم ورک Django
کنترل دسترسی	با استفاده از ایجاد Group و عضو کردن کاربران در گروه‌های خاص
دسترسی به نقشه‌ها با استفاده از GeoServer	Map Server

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 5, April 2017
انطباق با SFRها (قسمت دوم از CC)	توسعه یافته
انطباق با SARها (قسمت سوم از CC)	منطبق

۲-۲- انطباق با پروفایل حفاظتی

نام پروفایل حفاظتی	برنامه‌های کاربردی تحت شبکه نسخه ۱,۱ اسفندماه ۹۶

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	EAL1

۳- تعریف مسائل امنیتی

۳-۱- خط‌مشی

خط‌مشی	توصیف
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.
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. 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، پورت های 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.
P.E_SIGNATURE	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳-۲- تهدیدات

تهدیدات	توصیف
T.UNAUTHORIZED_ACCESS	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.

تهدیدات	توصیف
	مهاجم می‌تواند با سود بردن از نقض های 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.
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. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
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.
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

تهدیدات	توصیف
	ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می‌تواند عمداً یا غیر عمد موجب افشـــاء اطلاعات محرمانه گردد.
T.DENIAL_OF_SERVICE	مهاجم می‌تواند ســـبب گردد محصـــول 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 مشـخص می‌باشـد که به نام حمله DoS شـناخته می‌شـود. نوع دیگر پیشـرفته‌تر حمله DDoS می‌باشـد که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
T.HARMFUL_DATA	مهاجم می‌تواند یک رکورد، سـند یا داده مضـر را در داخل محصـول وارد نماید. با اســـتفاده 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.
T.ELEVATION_OF_PRIVILEGES	مهاجم می‌تواند با سـود بردن از دسـترسـی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.
T.NETWORK_EAVESDROP	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حســـاس بین محصـــول و مقصـــد موردنظر را مورد 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
A.TRUSTED_ADMIN	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
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.
A.EXPERIENCED_ DEVELOPER	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی دا شته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
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.
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.
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.

فرضیات	توصیف
A.SECURE_DELIVERY	فرض شـــده اســـت که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.
A.DIST_DENIAL_OF_SERVICE	فرض شـــده اســـت که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
O.AUDIT	محصـول باید هر رخدادی که در زمینه امنیتی دارای ارزش اسـت 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.
O.AUTH	محصـــول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصـــول 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 مســـتندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصـــول باید برای کاربران به صـــورت 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.

هدف امنیتی	توصیف
	از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت براســـاس توکن، احرازهویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
O.DATA_FLOW_CONTROL	محصـــول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواســت‌ها از یک رنج IP تعریف شــده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شـــبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
O.DATA_INTEGRITY	محصـــول باید نســـبت به صـــحت داده ممیزی و داده‌ی رکورد با تشـخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصـل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
O.MANAGEMENT	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد ســیســتم فراهم نماید. محصــول باید ســازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط‌های مدیریتی در نظر گیرد. محصــول باید برای مدیر ســیســتم 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.
O.ERROR_MANAGEMENT	محصول باید صورت امن و کارامد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصـول باید به کاربر به صـورت 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 برگشـــتی باید منجر به اقدام مناســـب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.

هدف امنیتی	توصیف
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.
O.TLS_COMMUNICATION	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۲-۴- اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
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.
OE.COMMUNICATION	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.
OE.TRUSTED_ADMIN	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
OE.TRUSTED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
OE.EXPERIENCED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده‌ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات

هدف امنیتی	توصیف
	مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.
OE.COMPLEMENTARY_AUDIT	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.
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.
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- نیازمندی‌های امنیتی

۵-۱- الزامات کارکرد امنیتی

عملیات انتخاب درون براکت و به صورت underlined و عملیات اختصاص درون براکت و با استایل bold نمایش داده خواهند شد. الزامات این قسمت از بخش پروفایل حفاظتی مرجع آورده شده.

شماره المان	نام کلاس	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		مرتبط نمودن هویت کاربر به رویداد ۱	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 محدود ۱	FAU_SAR.2.1
۷	**کلاس ممیزی امنیت**	بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.3.1
۸		انتخاب داده ممیزی ۱	FAU_SEL.1.1
۹		ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۱۰		ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۱۱		اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1
۱۲		پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱	FAU_STG.4.1
۱۳	**کلاس پشتیبانی از رمزنگاری**	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۴		عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۵		خط‌مشی کنترل دسترسی ۱	FDP_ACC.1.1
۱۶		عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۱۷		عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۱۸		عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۱۹		عملیات کنترل دسترسی ۴	FDP_ACF.1.4
۲۰		حفاظت کامل از اطلاعات باقیمانده در منابع ۱	FDP_RIP.2.1
۲۱		صحت داده کاربری ذخیره شده ۲	FDP_SDI.2.1
۲۲	**کلاس حفاظت از داده‌های کاربری**	صحت داده کاربری ذخیره شده ۳	FDP_SDI.2.2
۲۳		مدیریت احرازهویت ناموفق ۱	FIA_AFL.1.1
۲۴		مدیریت احرازهویت ناموفق ۲	FIA_AFL.1.2
۲۵		تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۲۶		مدیریت کلمه عبور (**FIA_SOS.1**)	FIA_PMG_EXT.1.1
۲۷	**کلاس شناسایی و احرازهویت**	احرازهویت کاربر ۱	FIA_UAU.1.1
۲۸		احرازهویت کاربر ۲	FIA_UAU.1.2
۲۹		سازوکار احرازهویت چندگانه ۱ (احرازهویت کاربر ۷)	FIA_UAU.5.1
۳۰		سازوکار احرازهویت چندگانه ۲ (احرازهویت کاربر ۸)	FIA_UAU.5.2
۳۱		شناسایی کاربر ۱	FIA_UID.1.1

۳۲		شناسایی کاربر ۲	FIA_UID.1.2
۳۳		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۳۴		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۳۵		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۳۶	**کلاس مدیریت امنیت**	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۳۷		مدیریت مشخصه‌های امنیتی ۱	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 داده‌های محصول ۱-مدیر سیستم	FMT_MTD.1.1 (1)
۴۱		مدیریت داده‌های 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	**کلاس حفاظت از توابع امنیتی محصول**	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۴۶		انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۴۷		سازگاری داده امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۴۸		سازگاری داده امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.1.2
۴۹		مهرهای زمانی ۱	FPT_STM.1.1
۵۰		به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۵۱	**کلاس تخصیص منابع**	تحمل خطا ۱	FRU_FLT.1.1
۵۲		محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۳		محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
۵۴		خاتمه دادن به نشست‌ها توسط محصول ۱	FTA_SSL.3.1
۵۵		خاتمه دادن به نشست‌ها توسط کاربر ۱	FTA_SSL.4.1
۵۶		سوابق دسترسی به محصول ۱	FTA_TAH.1.1

۵۷	**کلاس دسترسی به محصول**	سوابق دسترسی به محصول ۲	FTA_TAH.1.2
۵۸		سوابق دسترسی به محصول ۳	FTA_TAH.1.3
۵۹		برقراری نشست ۱	FTA_TSE.1.1
۶۰	**کلاس کانال‌ها/مسیرهای مورد اعتماد**	کانال امن ۱	FTP_ITC.1.1
۶۱		کانال امن ۲	FTP_ITC.1.2
۶۲		کانال امن ۳	FTP_ITC.1.3
۶۳		مسیر امن ۱	FTP_TRP.1.1
۶۴		مسیر امن ۲	FTP_TRP.1.2
۶۵		مسیر امن ۳	FTP_TRP.1.3
	الزامات پیوست ۱		
۶۶	**الزامات پیوست ۱ (پشتیبانی از رمزنگاری)**	تولید کلید رمزنگاری ۱	FCS_CKM.1.1
۶۷		تخریب کلید رمزنگاری ۱	FCS_CKM.4.1
۶۸		عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱ (۳)	FCS_COP.1.1(3)
۶۹		عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
	الزامات پیوست ۲(الزامات مبتنی بر انتخاب)		
۷۰	**کلاس پشتیبانی از رمزنگاری**	الزامات پروتکل HTTPS (۱)	FCS_HTTPS_EXT.1.1
۷۱		الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۷۲		الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۷۳		الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۷۴		الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۷۵		الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۷۶		الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۷۷		الزامات پروتکل TLS Server/احراز هویت ۱	FCS_TLSS_EXT.1.1
۷۸		الزامات پروتکل TLS Server/احراز هویت ۲	FCS_TLSS_EXT.1.2
۷۹		الزامات پروتکل TLS Server/احراز هویت ۳	FCS_TLSS_EXT.1.3
۸۰		الزامات پروتکل TLS Server/احرازهویت دو طرفه ۴	FCS_TLSS_EXT.2.4
۸۱		الزامات پروتکل TLS Server/احرازهویت دو طرفه ۵	FCS_TLSS_EXT.2.5
۸۲		الزامات پروتکل TLS Server/احرازهویت دو طرفه ۶	FCS_TLSS_EXT.2.6
۸۳	**(کلاس شناسایی و احرازهویت)**	الزامات پروتکل X509 (۱)/ ابطال	FIA_X509_EXT.1.1/Rev
۸۴		الزامات پروتکل X509 (۲)/ ابطال	FIA_X509_EXT.1.2/Rev
۸۵		الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۸۶		الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2

۱-۱-۵- کلاس ممیزی امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_GEN.1	FPT_STM.1 -	۱	FAU_GEN.1.1	**تولید داده ممیزی ۱:** محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید: • آغاز و اتمام توابع ممیزی؛ • تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول ۱ آمده است.

جدول۱- لیست رویدادهای قابل ممیزی

مولفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد ۱	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی ۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی‌که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
				پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱	عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
				صحت داده‌های کاربری ذخیره شده ۲	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
				احراز هویت کاربر	ثبت کاربرد ناموفق از سازوکار احراز هویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
				ساز و کار احراز هویت چندگانه	ثبت نتایج احراز هویت (حداقل) ثبت هر ساز و کار احراز هویت فعال همراه با نتیجه نهائی (پایه)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال
				مدیریت کلمه عبور	ثبت رد هر کلمه عبور تست شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
				انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
				مدیریت مشخصه‌های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				مدیریت داده‌های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
				مدیریت داده‌های محصول ۱-کاربرعادی، واردکننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
				عملیات رمزنگاری ۱ (۱)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
				عملیات رمزنگاری ۱ (۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				عملیات کنترل دسترسی ۱	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	شناسایی داده‌های موجودیت غیرفعال
				ورود داده‌های کاربری به محصول با مشخصه امنیتی	ورود داده کاربری موفقیت آمیز، شامل هر گونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	
				خروج داده‌های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج‌کردن اطلاعات از محصول (پایه)	
				مدیریت کارکرد در محصول	تمامی تغییرات در رفتارهای کارکردی محصول	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				کارکردهای مدیریتی محصول	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
				نقش‌های امنیتی	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش می‌باشد (حداقل)	
				سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	
				حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)	
				تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست می‌باشد (پایه)	
				برقراری نشست ۱	ثبت منع آغاز نشست به دلیل مکانیزم آغاز نشست (حداقل)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه) / محدودیت بر روی چندین نشست هم‌زمان: ثبت رد یک نشست مبتنی بر محدودیت نشست‌های هم‌زمان (حداقل) / خاتمه دادن به نشست‌ها: ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)
		۲	FAU_GEN.1.2	**تولید داده ممیزی ۲:** محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: • تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد • **[رخداد، نام کاربری، کد وضعیت، نوع درخواست، تاریخ ایجاد، آدرس IP، آدرس، دستگاه، توضیحات]**
FAU_GEN.2	- **FAU_GEN.1** - **FIA_UID.1**	۳	**FAU_GEN.2.1**	**مرتبط نمودن هویت کاربر به رویداد ۱:** برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_SAR.1	- FAU_GEN.1	۴	FAU_SAR.1.1	**بازبینی داده ممیزی ۱:** محصول باید امکان خواندن **[تاریخ شروع و پایان، آدرس IP، نوع درخوا ست (Get، Post و ...)، کد و ضعیت پا سخ (کدهای خطاهای وب سرویس)، انتخاب کاربران]**از کل رکوردهای ممیزی را برای **[پشتیبان سیستم و سایر کاربران با تعیین سطح دسترسی**] فراهم نماید.
FAU_SAR.1		۵	FAU_SAR.1.2	**بازبینی داده ممیزی ۲:** محصول باید رکوردهای ممیزی را طوری فراهم نماید که کاربر بتواند آن‌ها را درک و اطلاعات این رکوردها را تفسیر نماید.
FAU_SAR.2	- FAU_SAR.1	۶	FAU_SAR.2.1	**بازبینی داده ممیزی محدود ۱:** مح صول باید مانع د ستر سی خواندن رکوردهای ممیزی تو سط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.
FAU_SAR.3		۷	FAU_SAR.3.1	**بازبینی داده ممیزی قا بل انتخاب ۱:** محصول با ید امکان انجام **[م تدهای انتخاب و مرتب‌سازی]** رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس [**رخداد، نام کاربری، کد وضعیت، نوع درخواست، تاریخ ایجاد، آدرس IP، آدرس و [هیچ پارامتر دیگر]]** مرتب نماید.
FAU_SEL.1	- FAU_GEN.1 - FMT_MTD.1	۸	FAU_SEL.1.1	**انتخاب داده ممیزی ۱:** محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید: • **[هویت موجودیت فعال(شناسه کاربری)، نوع رخداد]** • **[پیام رخداد، پیام گزارش، آدرس، نوع درخوا ست (Get، Post و ...)، تاریخ شروع و پا یان، آدرس IP، جزئیات گزارش، نسخه سیستم عا مل، کد وضعیت (موفقیت‌آمیز، نیازمند احراز هویت و ...)]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_STG.1	- FAU_GEN.1	۹	FAU_STG.1.1	**ذخیره‌سازی رویدادهای ممیزی ۱:** محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید.
FAU_STG.1		۱۰	FAU_STG.1.2	**ذخیره‌سازی رویدادهای ممیزی ۲:** محصول باید قادر به [تشخیص و جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد.
FAU_STG.3	- FAU_STG.1	۱۱	FAU_STG.3.1	**اقدامات لازم در زمان از د ست رفتن داده ممیزی ۱:** محصول در صورت تجاوز دنباله ممیزی از [**یک محدودیت از پیش تعریف شده**] باید [**با استفاده از یک کانال ارتباطی مانند ایمیل ، از طریق واسطهای محصول و ارسال ایمیل به صورت متناوب کاربران مربوطه**] را مطلع نماید.
FAU_STG.4		۱۲	FAU_STG.4.1	**پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱:** محصول در صورت پر شدن دنباله ممیزی، [روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده دوباره‌نویسی می‌نماید] و [**برای هشدار از پر شدن فضای ذخیره سازی "به مدیر سیستم از طریق واسط کاربری و نیز ارسال ایمیل اطلاع داده شود.**].

۲-۱-۵- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.1	- [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] - FCS_CKM.4	۱۳	FCS_COP.1.1(1)	**عملیات رمزنگاری ۱ (۱):** محصول باید [**برای وارسی صحت داده‌های ممیزی و داده‌های رکورد**] بر اساس یک الگوریتم رمزنگاری مشخص [**الگوریتم رمزنگاری AES**] و اندازه کلید رمزنگاری [**256**] اجرا شود که مطابق با [**استاندارد** Rijndael] باشد.
FCS_COP.1		۱۴	FCS_COP.1.1(2)	**عملیات رمزنگاری ۱ (۲):** محصول باید [**برای تولید داده درهم‌سازی**] بر اساس مجموعه الگوریتم های رمزنگاری مشخص [**الگوریتم های رمزنگاری SHA-256**] و اندازه کلید رمزنگاری [**هیچ کدام**] اجرا شود که مطابق با [**SHA-256**] باشد.

۳-۱-۵- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_AFL.1	- FDP_ACF.1	۱۵	FIA_AFL.1.1	**مدیریت احرازهویت ناموفق ۱:** محصول باید بتواند با استفاده از [یک عدد مثبت قابل تنظیم توسط مدیر **[۱ الی N]**]، تلاش‌های ناموفق احرازهویت مرتبط با **[احراز هویت کاربر در هنگام ورود به سامانه]** را تشخیص دهد.
FIA_AFL.1	- FDP_ACC.1 - FMT_MSA.3	۱۶	FIA_AFL.1.2	**مدیریت احرازهویت ناموفق ۲:** زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [بیشتر از حد تعیین شده رسید] ، محصول باید **[مکانیزم قفل شدن IP کاربر]** را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_ATD.1		۱۷	**FIA_ATD.1.1**	**تعریف م شخ صات کاربر ۱:** محصـول باید مشـخصـه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: [• **شناسه کاربر** • **متد احرازهویت مورد استفاده** • **داده احرازهویت** • **نقش کاربر** • **وضعیت حساب کاربری (فعال، غیرفعال بلوکه شده و غیره)** • **[هیچ مشخصه امنیتی دیگر]**]
FIA_PMG_EXT.1		۱۸	**FIA_PMG_EXT.1.1**	**مدیریت کلمه عبور:** محصول باید قابلیت‌های مدیریت کلمه عبور را که در زیر ذکر شده‌اند برای کلمه‌های عبور مدیریتی فراهم نماید: ۱. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: ["@"، "$"، "٪"، "!" "&"، "*" و **[هیچ کاراکتر دیگری]]** باشد. ۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.
FIA_UAU.1		۱۹	**FIA_UAU.1.1**	محصول باید پیش از احراز هویت کاربر، اجازه اقدامات میانی زیر را به کاربر دهد: [

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• مشاهده راهنمای نحوه ورود به سیستم • شناسایی کاربر • بازیابی کلمه‌عبور (فقط مدیر سیستم)]
FIA_UAU.1		**۲۰**	**FIA_UAU.1.2**	**احرازهویت کاربر ۲:** محصول باید هر کاربر را پیش از آن‌که امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت نماید.
FIA_UAU.5	**- [FDP_ACC.1, or FDP_IFC.1]** **- [FTP_ITC.1, or FTP_TRP.1]** **- FPT_TDC.1**	**۲۱**	**FIA_UAU.5.1**	**سازوکار احرازهویت چندگانه ۱:** محصول باید به منظور احرازهویت کاربر ساز و کارهای زیر را فراهم آورد:] • **نام کاربری و کلمه عبور** • **[از طریق ایمیل]** [
FIA_UAU.5		**۲۲**	**FIA_UAU.5.2**	**سازوکار احرازهویت چندگانه ۲:** محصول باید هر کاربر متقاضی احرازهویت را مطابق ذیل احرازهویت نماید.] • **کاربران از راه‌دور باید علاوه بر برر سی نام کاربری و کلمه عبور از روش احرازهویت چندگانه (مانند Dual factor authentication) استفاده کند.** • **[از طریق ایمیل]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[
FIA_UAU.5		۲۳	FIA_UID.1.1	**شناسایی کاربر ۱:** محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: [• **مشاوره راهنمای نحوه ورود به سیستم** • **ورود به صورت مهمان]**]
FIA_UAU.5		۲۴	FIA_UID.1.2	**شناسایی کاربر ۲:** توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی نماید.
FIA_USB.1		۲۵	FIA_USB.1.1	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱:** محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: [• **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)** • **[آدرس IP کاربری و زمان و تاریخ آخرین ورود کاربر]**]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_USB.1	- [FDP_ACC.1, or FDP_IFC.1]	۲۶	FIA_USB.1.2	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲:** محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید: [• **زمانی که یک نشست جدید برقرار می شود، اعتبار نشست‌های 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.** • **[زمان‌دار بودن نشست]**]
FIA_USB.1		۲۷	FIA_USB.1.3	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳:** محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه¬های امنیتی کاربر فعال اعمال نماید: • **[هیچ تغییری در طول نشست فعال مجاز نمی‌باشد** • **[دیگر قوانین حاکم بر تغییرات مشخصه‌ها مانند منوهای سیستم در هر بار فراخوانی سرور بر اساس آخرین وضعیت نقشهای کاربر بروزآوری**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				شده و نمایش داده می شوند، تمام قوانین امنیتی موجود در فریم ورک Django می‌باشد]]

۴-۱-۵- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1	- **[FDP_ACC.1, or FDP_IFC.1]**	**۲۸**	**FDP_ACC.1.1**	**خط‌مشی کنترل دسترسی ۱:** محصول باید **[خط‌مشی‌های کنترل دسترسی]** را بر روی موارد زیر اعمال نماید:] • **موجودیت فعال: [مدیر سیستم، کاربر عادی، [کاربر مهمان]** • **موجودیت غیرفعال:** ○ **رکوردها، مستندات و فرا-داده** ○ **داده متعلق به کاربران** ○ **داده احرازهویت** ○ **داده با این معیارها: [هیچ معیار دیگری]** ○ **[هیچ موجودیت‌های غیر فعال دیگری]** • **عملیات:**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ **ایجاد موجودیت غیرفعال جدید** ○ **حذف موجودیت غیرفعال** ○ **تغییر دسترسی‌ها به موجودیت غیرفعال** ○ **عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال** ○ [**هیچ عملیات دیگری**]]
FDP_ACF.1		**۲۹**	**FDP_ACF.1.1**	**عملیات کنترل د ستر سی ۱:** محصول باید [**خط‌مشی‌های کنترل د ستر سی**] 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** • [**هیچ مشخصه ی موجودیت غیرفعال دیگری**]]
FDP_ACF.1	-	**۳۰**	**FDP_ACF.1.2**	**عملیات کنترل دســترســی ۲:** محصــول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[**عملیات تنها به شرطی مجاز ا ست که در لی ست کنترل د ستر سی، رکوردی وجود دا شته با شد که به کاربر با شنا سه کاربری یا شنا سه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.**]
FDP_ACF.1	-	۳۱	**FDP_ACF.1.3**	**عملیات کنترل د ستر سی ۳:** مح صول باید برا ساس قوانین زیر، د ستر سی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: [• **کاربران با مجوز مدیر سی ستم به رکوردهای لازمه مدیریت سی ستم و نیز روش ارائه شده توسط محصول، دسترسی دارند.** • **کاربران غیر مجاز بدون نیاز به فرآیند احراز هو یت، به اطلاعات قابل دسترس عموم، دسترسی دارند.** • **[هیچ قانون دیگری]**]
FDP_ACF.1	**FIA_UAU.1** -	۳۲	**FDP_ACF.1.4**	**عملیات کنترل د ستر سی ۴:** مح صول باید صراحتا بر ا ساس قوانین زیر از د ستر سی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: [• **تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده** • **[هیچ قانون دیگری]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[
FDP_RIP.2		**۳۳**	**FDP_RIP.2.1**	**حفاظت کامل از اطلاعات باقیمانده در منابع ۱:** محصول باید تضمین نماید در هنگام [تخصیص منابع به یا آزادسازی منابع از] تمام موجودیت‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.
FDP_ETC.2	- **FIA_ATD.1**	**۳۴**	**FDP_SDI.2.1**	**صحت داده کاربری ذخیره شده ۲:** محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص [**خطاهای صحت داده**] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های [**درهم شده داده‌های کاربری ذخیره شده**] پایش نماید.
FDP_SDI.2		**۳۵**	**FDP_SDI.2.2**	**صحت داده کاربری ذخیره شده ۳:** هنگام تشخیص خطای صحت داده، محصول باید [**اطلاع به کاربر و ممانعت از ثبت داده**] را صورت دهد.

۵-۱-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.1	- FMT_SMR.1 - FMT_SMF.1	۳۶	FMT_MOF.1.1	**مدیریت کارکرد در محصول ۱:** محصول باید امکان [تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] توابع [**تمام کارکردهای مربوط به مدیریت محصول**] را به [**مدیر سیستم و هر کاربری که مجوز لازم را دارد**، [**هیچ نقش دیگر**]] محدود نماید.
FMT_MOF.1	- [FDP_ACC.1, or FDP_IFC.1] - FMT_SMR.1 - FMT_SMF.1	۳۷	FMT_MSA.1.1	**مدیریت مشخصه‌های امنیتی ۱:** محصول باید با اعمال [**خطمشی کنترل دسترسی**]، امکان تغییر پیش‌فرض، [پرس و جو، تغییر، حذف، [**هیچ عملیات دیگر**]] مشخصه‌های امنیتی [• **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)** • [**آدرس IP کاربری و زمان و تاریخ آخرین ورود کاربر**]] را به [**مدیر سیستم و هر کاربری که مجوز لازم را دارد**] محدود نماید.
FMT_MSA.3	- FMT_MSA.1 - FMT_SMR.1	۳۸	FMT_MSA.3.1	**مدیریت مشخصه‌های امنیتی ۳:** محصول برای مشخصه‌های امنیتی که برای اعمال [**خط مشی**] استفاده می‌شوند، باید مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MSA.3		۳۹	FMT_MSA.3.2	**مدیریت مشخصه‌های امنیتی ۴:** 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.
FMT_MTD.1	- FMT_SMR.1 - FMT_SMF.1	۴۰	FMT_MTD.1.1 (1)	**مدیریت داده‌های محصول ۱ – مدیر سیستم (۱):** محصول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [**[هیچ کارکرد دیگری]]** [**لیستی از داده‌های محصول مانند رویدادهای ممیزی، داده‌های احراز هویت و تنظیمات امنیتی**] به [**مدیر سیستم، [کاربری که مدیر سیستم به او دسترسی داده است]]** محدود نماید.
FMT_MTD.1		۴۱	FMT_MTD.1.1 (2)	**مدیریت داده‌های محصول کاربر عادی، وارد کننده داده (۲):** محصول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، [**هیچ کارکرد دیگری]]** [**لیستی از داده های محصول مانند پسورد کاربر، شماره‌ی تماس و یا آدرس ایمیل (که برای مقا صد امنیتی نظیر بازیابی رمز عبور و یا ار سال رمز یک‌بار مصرف**] به [**مدیر سیستم، [هیچ نقش دیگری]]** محدود نماید.
FMT_SMF.1	-	۴۲	FMT_SMF.1.1	**کارکردهای مدیریتی محصول ۱:** محصول باید قادر به انجام [**کارکردهای مدیریتی که در جدول زیر آمده است**] باشد:

مؤلفه	وابستگی ها	شماره	المان	شرح المان

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
اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده در منابع	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پیکربندی باشد.
ورود داده‌های کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده‌های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاش‌های ناموفق

مؤلفه	وابستگی ها	شماره	المان	شرح المان	
					مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
				تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد. [اختیاری]
				مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت‌ها برای تنظیم کلمه عبورها
				احراز هویت کاربر	مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احراز هویت کاربر انجام می‌شوند.
				سازوکار احراز هویت چندگانه	مدیریت ساز و کارهای احراز هویت مدیریت قوانین مرتبط با احراز هویت
				شناسایی کاربر	مدیریت شناسایی کاربران [اختیاری] مدیریت تغییرات و فرآیندهایی مانند (اختصاص ادرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.
				انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و تغییر دهد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				مدیریت مشخصه‌های امنیتی: مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند. مقدار دهی اولیه مشخصه‌ها: مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول مدیریت داده‌های محصول ۱- مدیر سیستم: مدیریت گروهی از قوانینی مرتبط با داده‌های محصول مدیریت داده‌های محصول ۱- کاربرعادی، وارد کننده داده: مدیریت گروهی از قوانینی مرتبط با داده‌های محصول نقش‌های امنیتی: مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند. محدودیت بر روی چندین نشست هم‌زمان: مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر برقراری نشست: مدیریت شرایط آغاز نشست توسط مدیر مجاز خاتمه دادن به نشست‌ها: تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.
FMT_SMR.1	FIA_UID.1 -	۴۳	FMT_SMR.1.1	**نقش‌های امنیتی ۱:** نقش‌های زیر در محصول باید تعریف شده باشد:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[مدیر سیستم **[مهمان]**]
FMT_SMR.1		**۴۴**	**FMT_SMR.1.2**	**نقش های امنیتی ۲:** محصـــول، باید قادر به مرتبط نمودن کاربران با نقش ها و دسترسی‌های مجاز تعریف شده باشند.

۶-۱-۵- کلاس حفاظت از توابع امنیتی هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.1	-	۴۵	FPT_FLS.1.1	**حفظ وضعیت امن در زمان شکست ۱:** محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: **[شکست‌های نرم‌افزاری، شکست‌های سخت‌افزاری]**
FPT_ITT.1	-	۴۶	FPT_ITT.1.1	**انتقال داده امنیتی در داخل محصول ۱:** محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیر ساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که باهم ارتباط دارند، محافظت نماید.
FPT_TDC.1	-	۴۷	FPT_TDC.1.1	**سازگاری داده امنیتی بین محصول و موجودیت امن ۱:** محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار **[کدهای یک‌بار مصرف ارسال شده به سرور پست الکترونیکی]** را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد.
FPT_TDC.1		۴۸	FPT_TDC.1.2	**سازگاری داده امنیتی بین محصول و موجودیت امن ۲:** محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، **[لیستی از قوانین تفسیر که در محصول به کار می‌روند مانند پروتکل‌های OGC در ارتباط با سرور مکانی جهت ارسال داده‌های مکانی مورد استفاده قرار می‌گیرد، API]** استفاده نماید.
FPT_STM.1	افتا -	۴۹	FPT_STM.1.1	**مهر های زمانی:** توابع امنیتی هدف ارزیابی باید قادر به ایجاد مهر های زمانی قابل اطمینان باشند.

FPT_TUD_EXT.1	**افتا** -	**۵۰**	**FPT_TUD_EXT.1.2**	**به روز رسانی امن ۲:** محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کار شناس شرکت تولیدکننده محصول فراهم نماید که به‌روز سانی نرم‌افزار و میان‌افزارمحصول مورد ارزیابی را به صورت دستی آغاز نماید و [از مکانیزم بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی].

۷-۱-۵- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.1	**FPT_FLS.1** -	**۵۱**	**FRU_FLT.1.1**	**تحمل خطا ۱:** محصول باید از عملکرد [**تمام کارکردهای اصلی**] هنگام رویداد شکست‌های زیر اطمینان حاصل نماید: [**شکست نرم‌افزاری، هیچ شکست دیگری**]]

۸-۱-۵- کلاس دسترسی به هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_MCS.1	FIA_UID.1 -	۵۲	FTA_MCS.1.1	**محدودیت بر روی چندین نشست همزمان ۱:** محصول باید حداکثر تعداد نشست‌های هم‌زمان متعلق به یک کاربر را محدود نماید.
FTA_MCS.1		۵۳	FTA_MCS.1.2	**محدودیت بر روی چندین نشست همزمان ۲:** محصول باید به صورت پیش‌فرض، [**پیش‌فرض عدد ∞ و قابل تنظیم توسط مدیر سیستم**] برای هر کاربر در نظر بگیرد.
FTA_SSL.3	-	۵۴	FTA_SSL.3.1	**خاتمه دادن به نشست ها توسط محصول ۱:** محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمان [**بازه زمانی که توسط مدیرتنظیم می‌شود**] غیرفعال بودن، خاتمه دهد.
FTA_SSL.4	-	۵۵	FTA_SSL.4.1	**خاتمه دادن به نشست ها توسط کاربر ۱:** محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.
FTA_TAH.1	-	۵۶	FTA_TAH.1.1	**سوابق دسترسی به محصول ۱:** در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [روز، زمان، **IP**] باشد.
FTA_TAH.1		۵۷	FTA_TAH.1.2	**سوابق دسترسی به محصول ۲:** در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید [تاریخ، زمان] آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش‌های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_TAH.1		۵۸	FTA_TAH.1.3	**سوابق د ستر سی به مح صول ۳:** توابع امنیتی هدف ارزیابی نباید اطلاعات تاریخچه دسترسی را از واسط کاربری پاک نماید، بدون این‌که به کاربر فرصتی داده شود تا اطلاعات را بازبینی نماید.
FTA_TSE.1	-	۵۹	FTA_TSE.1.1	**برقراری نشست ۱:** توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس [**مکان، شماره پورت، تعداد تلاش‌های ناموفق احرازهویت، شنا سه کاربر(نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP** [**هیچ مشخصه دیگر**]] ممانعت نماید.

۹-۱-۵- کلاس کانال‌ها و مسیرهای مورد اعتماد

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.1	افتا -	۶۰	FTP_TRP.1.1	**مسیر امن ۱:** محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [TLS, HTTPS] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد.
FTP_TRP.1	افتا -	۶۱	FTP_TRP.1.2	**مسیر امن ۲:** محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.1	**افتا** -	**۶۲**	**FTP_TRP.1.3**	**مسیر امن ۳:** محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی نماید.
	افتا -	**۶۳**	**FTP_ITC.1.1**	**کانال امن ۱:** محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [HTTPS,TLS] میان خود و موجودیت IT معتبر، سرور ممیزی، [سرور ممیزی، **[پایگاه داده، GeoServer]]** 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.
	افتا -	**۶۴**	**FTP_ITC.1.2**	**کانال امن ۲:** محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.
	افتا -	**۶۵**	**FTP_ITC.1.3**	**کانال امن ۳:** محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [**تمامی خدمات**] راه‌اندازی نماید.

۱۰-۱-۵- الزامات کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_CKM.1		**۶۶**	**FCS_CKM.1.1**	**تولید کلید رمزنگاری ۱:** محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر تولید کنند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[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.]
FCS_CKM.4		۶۷	**FCS_CKM.4.1**	**تخریب کلید رمزنگاری ۱:** محصول باید براساس متد تخریب کلید رمزنگاری **[با استفاده از کتابخانه Shred]** که بر اساس استاندارد **[** • **United States Department of Defense 5220.22-M National IndustrialSecurity Standard** • **Germany BSI Verschlusssachen-IT-Richtlinien** • **Bruce Schneier's Algorithm** • **Peter Gutmann's Algorithm RCMP DSX Method** **]** باشد، کلیدهای رمزنگاری را از بین ببرد.
FCS_COP.1		۶۸	**FCS_COP.1.1(3)**	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۳):** محصول باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری متقارن AES- XTS مطابق مستند NIST SP 800- 38E, AES-CBC مطابق سند NIST SP 800- 38A و [AES-CCM مطابق سند NIST SP 800-38C] با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.

۱۱-۱-۵- الزامات پروتکل HTTPS

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_HTTPS_EXT.1		۶۹	FCS_HTTPS_EXT.1.1	**الزامات پروتکل HTTPS (۱):** محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.
		۷۰	FCS_HTTPS_EXT.1.2	**الزامات پروتکل HTTPS (۲):** محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.
	افتا -	۷۱	FCS_HTTPS_EXT.1.3	**الزامات پروتکل HTTPS (۳):** در صورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [اتصال را برقرار ننماید].

۱۲-۱-۵-الزامات پروتکل TLS Client

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_TLSC_EXT.1		۷۲	FCS_TLSC_EXT.1.1	**الزامات پروتکل TLS Client (۱):** محصول باید [TLS 1.2 (RFC 5246)] را پیاده‌سازی کند و دیگر نسخه های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: [TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246]
FCS_TLSC_EXT.1		۷۳	FCS_TLSC_EXT.1.2	**الزامات پروتکل TLS Client (۲):** محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_TLSC_ EXT.1		**۷۴**	**FCS_TLSC_EXT.1.3**	**الزامات پروتکل TLS Client (۳):** 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، **[هیچ اقدام دیگری]**].
FCS_TLSC_ EXT.1		**۷۵**	**FCS_TLSC_EXT.1.4**	**الزامات پروتکل TLS Client (۴):** محصول باید [Supported Elliptic Curves Extension را ارائه نکند و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.

۱۳-۱-۵-الزامات پروتکل TLS Server

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_TLSS_E XT.1		**۷۶**	**FCS_TLSS_EXT.1.1**	**الزامات پروتکلTLS Server (۱):** محصول باید [TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: [TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246]
FCS_TLSS_ EXT.1		**۷۷**	**FCS_TLSS_EXT.1.2**	**الزامات پروتکلTLS Server (۲):** محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [TLS1.1] دارند، رد نماید.
FCS_TLSS_ EXT.1		**۷۸**	**FCS_TLSS_EXT.1.3**	**الزامات پروتکلTLS Server (۳):** محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [هیچ اندازه دیگری] و [هیچ منحنی دیگری]، [هیچ اندازه دیگری] ایجاد نماید.

۲-۵- الزامات شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_X509_EXT.1		۷۹	**FIA_X509_EXT.1.1/Rev**	**الزامات پروتکل X509 (۱)/ ابطال:** محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است. • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [هیچ روش فسخی] تأیید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند: ○ گواهی‌نامه‌های مورداستفاده برای تأیید به‌روزرسانی‌های 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.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند. گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های 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.
FIA_X509_EXT.1		۸۰	**FIA_X509_EXT.1.2/Rev**	**الزامات پروتکل X509 (۲)/ ابطال:** محصـــول مورد ارزیابی تنها درصـــورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم شده با شد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.
FIA_X509_EXT.2		۸۱	**FIA_X509_EXT.2.1**	**الزامات پروتکل X509 (۳):** محصـــول مورد ارزیابی باید جهت پشـــتیبانی احرازهویت برای [TLS, HTTPS] و [**هیچ کاربرد دیگری**] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.
FIA_X509_EXT.2		۸۲	**FIA_X509_EXT.2.2**	**الزامات پروتکل X509 (۴):**در صـــورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشـــد، توابع امنیتی هدف ارزیابی باید [به مدیر سیستم این امکان را بدهد که در زمینه‌ی پذیرش گواهی تصمیم‌گیری نماید].

۳-۵- بخش توجیهات

مؤلفه	وابستگی	شماره	المان	شرح المان
FDP_ITC.2	- FIA_UID.1	۱	FDP_ITC.2.1	**ورود داده کاربری به محصول با مشخصه امنیتی ۱:** محصول باید هنگام دریافت داده کاربری، خط‌مشی کنترل دسترسی را اعمال نماید ولی با توجه به توضیحات در این استاندارد نمی‌گنجد.
FDP_ITC.2		۲	FDP_ITC.2.2	**ورود داده کاربری به محصول با مشخصه امنیتی ۲:** در این محصول چون تعداد نقشه‌ها متفاوت و نامحدود می‌باشد تعداد دفعات Import در نظر گرفته نمی‌شود.
FDP_ITC.2	-	۳	FDP_ITC.2.3	**ورود داده کاربری به محصول با مشخصه امنیتی ۳:** محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه‌های امنیتی و داده کاربری دریافت شده، فراهم می‌نماید ولی با توجه به توضیحات در این استاندارد نمی‌گنجد.
FDP_ITC.2	-	۴	FDP_ITC.2.4	**ورود داده کاربری به محصول با مشخصه امنیتی ۴:** محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، می‌باشد ولی با توجه به توضیحات در این استاندارد نمی‌گنجد.
FDP_ITC.2	-	۵	FDP_ITC.2.5	**ورود داده کاربری به محصول با مشخصه امنیتی ۵:** محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی را اعمال نماید ولی با توجه به توضیحات در این استاندارد نمی‌گنجد.
FDP_ETC.2	-	۶	FDP_ETC.2.1	**خروج داده کاربری از محصول با مشخصه امنیتی ۱:** محصول داده را به صورت متادیتا می‌فرستد و چون یک سری اطلاعات مشخص هست ولی الزام‌آور نیست، پس نیازی به موارد امنیتی ندارد.

FDP_ETC.2	-	۷	**FDP_ETC.2.2**	**خروج داده کاربری از محصول با مشخصه امنیتی ۲:** محصول داده را به صورت متادیتا می‌فرستد و چون یک سری اطلاعات مشخص هست ولی الزام‌آور نیست، پس نیازی به موارد امنیتی ندارد.
FDP_ETC.2	-	۸	**FDP_ETC.2.3**	**خروج داده کاربری از محصول با مشخصه امنیتی ۳:** محصول داده را به صورت متادیتا می‌فرستد و چون یک سری اطلاعات مشخص هست ولی الزام‌آور نیست، پس نیازی به موارد امنیتی ندارد.
FDP_ETC.2	- **FIA_ATD.1**	۹	**FDP_ETC.2.4**	**خروج داده کاربری از محصول با مشخصه امنیتی ۴:** محصول داده را به صورت متادیتا می‌فرستد و چون یک سری اطلاعات مشخص هست ولی الزام‌آور نیست، پس نیازی به موارد امنیتی ندارد.
FCS_COP.1		۱۰	**FCS_COP.1.1(4)**	**عملیات رمزنگاری ۱(۴):** محصول مورد ارزیابی باید خدمات امضای دیجیتال (تولید و تأیید) را بر اساس الگوریتم های رمزنگاری ارائه کند ولی با توجه به توضیحات، در این استاندارد نمی‌گنجد.
FPT_TUD_EXT.1	–	۱۱	**FPT_TUD_EXT.1.3**	**به روز رسانی امن ۳:** محصول دارای به روزرسانی خودکار نمی باشد. در نتیجه این الزام قابل اجرا نمی‌باشد.

۴-۵- الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف‌کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 براساس بخش سوم استاندارد ISO/IEC15408 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام مؤلفه	توضیحات
Development	**ADV_FSP.1**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.1**	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Security Target	**ASE_CCL.1**	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.1	اهداف امنیتی

	ASE_REQ.1	الزامات امنیتی معین
	ASE_TSS.1	خلاصه مشخصات هدف ارزیابی
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

۶- خلاصه مشخصات هدف ارزیابی

نسخه ۱,۵ سند هدف امنیتی سامانه مدیریت و یکپارچه‌سازی داده‌های مکانی ژئوتاژک نسخه ۳,۲,۲ توسط کمیته توسعه شرکت دانش‌بنیان سامانه‌های آزاد فناوری اطلاعات ایده‌آل آینده ایرانیان سافا تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

۱-۶- کلاس ممیزی امنیت

محصول می‌تواند 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 تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد، نوع کاربری، IPکاربر، 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_GEN.1.2, FAU_GEN.2.1)

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 مرتب‌سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را برا ساس مرکز برگزارکننده، کاربر، نوع کاربری، تاریخ، مو ضوع و نوع رخداد (عملیات) مرتب نماید. (FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_SAR.3.1)

محصول می‌تواند بر اساس مشخصه‌هایی مانند هویت موجودیت فعال(شناسه کاربری)، نوع رخداد، زمان رویداد، تاریخ و آدرس IP کاربر از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید. (FAU_SEL.1.1)

محصول می‌تواند رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید. همچنین قادر به تشخیص و جلوگیری تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی

آن‌ها می‌باشد. در صورت تجاوز دنباله ممیزی از یک محدودیت از پیش تعریف شده محصول با استفاده از یک کانال ارتباطی مانند ایمیل یا پیام کوتاه، از طریق واسط‌های محصول و ارسال ایمیل و ارسال پیامک (در صورت وجود سامانه پیامکی) به صورت متناوب کاربران مربوطه را مطلع می‌نماید. همچنین در صورت پر شدن دنباله ممیزی، محصول قادر است روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید و برای هشدار از پر شدن فضای ذخیره‌سازی به مدیر سیستم و پشتیبان از طریق واسط کاربری و نیز ارسال ایمیل اطلاع داده می‌شود. (FAU_STG.1.1, FAU_STG.1.2, FAU_STG.3.1, FAU_STG.4.1)

می‌توان بر اساس مشخصه‌های شعبه، گروه کاربری، محدوده زمانی، موضوع، فرم و IP مجموعه از رویدادها را جهت ممیزی نمودن انتخاب نمود.

۲-۶- کلاس پشتیبانی از رمزنگاری

محصول می‌تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد " استفاده از طرح RSA با اندازه کلید ۱۰۴۸ بیت یا بیشتر که از اسناد PUB 186FIPS-4 ، .Standard) DSS)" "Signature Digital ،" B 3Appendix پیروی می‌کند تولید کنند و رمزنگاری و رمزگشایی را مطابق با، F38-800NIST SP سند مطابق AES Key Wrap with Paddi ng (KWP متقارن رمزنگاری الگوریتم اندازه کلید رمزنگاری ۱۱۸ و ۱۹۶ بیتی را انجام دهد. (FCS_COP.1.1(1), FCS_COP.1.1(2))

۳-۶- کلاس شناسایی و احرازهویت

می‌توان با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش‌های احراز هویت ناموفق را مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد. (FIA_AFL.1.1, FIA_AFL.1.2)

محصول می‌تواند پیش از احرازهویت کاربر، اجازه اقدامات میانی مانند مشاهده راهنمای نحوه ورود به سیستم، شناسایی کاربر، بازیابی کلمه‌عبور (فقط مدیر سیستم) را به کاربر می‌دهد و هر کاربر را پیش از آن‌که امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت می‌نماید. (FIA_UAU.1.1, FIA_UAU.1.2, FIA_UID.1.1, FIA_UID.1.2)

محصول به منظور احرازهویت کاربر از سازوکار نام کاربری و کلمه عبور استفاده می‌کند که برای کاربران از راه‌دور علاوه بر بررسی نام کاربری و کلمه عبور از روش احرازهویت ازطریق ارسال ایمیل استفاده می‌کند. (FIA_UAU.5.1, FIA_UAU.5.2)

محصول باید مشخصه‌های امنیتی شناسه کاربر داده‌های 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. (FIA_ATD.1.1, FIA_PMG_EXT.1.1)

محصول می‌تواند مشخصه‌های امنیتی شناسه کاربر، نقش‌های کاربر، جزئیات 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. علاوه بر آن در تنظیمات سامانه می‌تواند موارد زیر را تعریف کرد:

مدت زمان توکن access: پس از سپری شدن این زمان، توکن کاربر دوباره اعتبار سنجی می‌شود.

مدت زمان توکن refresh: پس از سپری شدن این زمان، کاربر باید مجددا لاگین کند

مدت زمان تعامل نداشتن کاربر: اگر در کاربر به این مقدار دقیقه در سیستم فعالیتی انجام ندهد، نشست کاربر منقضی شده و باید مجددا لاگین کند (FIA_USB.1.1, FIA_USB.1.2, FIA_USB.1.3).

زمانی‌که یک نشست جدید برقرار می‌شود، اطلاعات موجود از نشست‌های قبلی حذف می‌گردد. اطلاعات پیشینه احراز هویت بروزرسانی می‌شود. رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید ثبت می‌گردد. (FIA_USB.1.1, FIA_USB.1.2, FIA_USB.1.3)

محصول با استفاده از خط‌مشی‌های کنترل دسترسی بر روی موجودیت‌های فعال (مدیر سیستم، کاربر عادی، کاربر مهمان) و موجودیت‌های غیرفعال (رکوردها، مستندات و فراداده، داده متعلق به کاربران، داده احرازهویت) عملیاتی مانند ایجاد موجودیت غیرفعال جدید، حذف موجودیت غیرفعال، تغییر دسترسی‌ها به موجودیت غیرفعال، عملیات بر روی فراداده وابسته به موجودیت غیرفعال را می‌تواند انجام دهد. (FDP_ACC_1.1)

امکان نگهداری داده کاربری حساس ذخیره شده در مکان تحت کنترل براساس مشخصه‌های رمزنگاری امن نگهداری کرده و آن‌ها را به منظور شناسایی خطای صحت داده رکورد و داده ممیزی پایش کند. (FIA_USB.1.1, FIA_USB.1.2, FIA_USB.1.3)

۴-۶- کلاس حفاظت از داده‌های کاربر

محصول می‌تواند داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص خطاهای صحت داده، و داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های درهم شده داده‌های کاربری ذخیره شده، پایش نماید. هنگام تشخیص خطای صحت داده، به کاربر اطلاع داده می‌شود و از ثبت داده ممانعت می نماید. جدول‌های account_user , layers_layer , roles_role , global_settings_globalsettings تحت این کنترل قرار گرفته‌اند.(FDP_SDI.2.1,FDP_SDI.2.2)

سیستم می‌تواند هنگام تشخیص خطای صحت داده ممیزی مربوطه را ثبت نماید.

محصول این امکان را فراهم می‌کند که کاربر مدیرسیستم و کاربرانی که دسترسی‌های لازم را دارند (باتوجه به سطح دسترسی‌شان) بتواند موجودیت غیرفعال (شامل رکوردها، مستندات، فرا-داده‌ها، داده متعلق به کاربران، داده احرازهویت)ی را ایجاد ویرایش و یا حذف کنند و یا دسترسی به آن‌ها را تغییر دهند. (FDP_ACC.1.1, FDP_ACF.1.3)

در سیستم دسترسی به کاربران به دو صورت دسترسی به کاربر و دسترسی به نقش تعریف می‌شود. کاربر به شرطی مجاز به استفاده از منابع دسترسی داده شده است که یا خود دارای دسترسی باشد و یا در نقش حاوی این دسترسی وجود داشته باشد (FDP_ACF.1.1, FDP_ACF.1.2).

محصول این قابلیت را دارد که در صورتیکه تعداد نشست‌هایی با یک نام کاربری مشابه به تعداد مشخصی رسید، اجازه ایجاد نشست جدیدی به کاربر داده ندهد. و تنها در صورت پایان نشست توسط مدیر سسیتم یا خروج هر یک از نشست ها یا اتمام زمان نشست و یا استفاده از گزینه بستن سایر نشست‌های همزمان در زمان ورود، اجازه ایجاد نشست جدید را می‌دهد. در صورت بسته شدن نشستی آن نشست غیرقابل دسترس می‌گردد (FDP_ACF.1.4, FDP_RIP.2.1).

محصول می‌تواند سطح دسترسی را با توجه به هویت کاربر، نقش‌ها و مجوزهای کاربر مجاز و اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند، بر روی موجودیت‌های 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 می‌باشد. (FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4)

می‌توان 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 نمود و امکان در نظرگرفتن مقادیر پیش‌فرض محدود شده محصول برای مشخصه‌های امنیتی که برای اعمال خط‌مشی استفاده می شوند، وجود داشته و مدیر سیستم از طریق فایل Config می‌تواند هنگام ایجاد اطالعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد. (FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4)

۵-۶- کلاس مدیریت امنیت

محصول امکان مدیریت کارکردها را دارد یعنی با استفاده از تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار توابع و ارائه تمام کارکردهای مربوط به مدیریت محصول به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدودیت ایجاد می‌نماید. (FMT_MOF.1.1)

محصول با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض، پرس و جو، تغییر و حذف مشخصه‌های امنیتی مانند شناسه کاربر، نقش‌ها، مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه، جزئیات واسط

کلاینت، پیشـــینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)، آدرس IP کاربری، زمان و تاریخ آخرین ورود کاربر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، را ایجاد می‌نماید. (FMT_MSA.1.1)

محصول برای مشخصه‌های امنیتی که برای اعمال خط‌مشی استفاده می‌شوند، مقادیر پیش‌فرض محدود شده‌ای را در نظر می‌گیرد. (FMT_MSA.3.1)

محصول برای تعیین مقادیر اولیه پیشنهادی به مدیر سیستم اجازه می‌دهد تا هنگام ایجاد اطلاعات یا موجودیت غیرفعال، مقادیر پیش‌فرض را لغو و تغییر دهد. (FMT_MSA.3.2)

محصـــول توانایی تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف و پاک نمودن لیســـتی از داده‌های محصـــول مانند رویدادهای ممیزی، داده‌های احراز هویت و تنظیمات امنیتی را به مدیر سـیسـتم یا کاربری که مدیر سـیسـتم به او دسترسی داده است، لیستی از داده‌های محصول مانند پسورد کاربر، شماره تماس و یا آدرس ایمیل (که برای مقاصد امنیتی نظیر بازیابی رمز عبور و یا ارسـال رمز یکبار مصـرف به مدیر سـیسـتم، را ایجاد می‌نماید. (FMT_MTD.1.1 (۱)، FMT_MTD.1.1 (۲))

محصول قادر به انجام کارکردهای مدیریتی مانند بازبینی داده ممیزی ۱، انتخاب داده ممیزی ۱، اقدامات لازم در زمان از دست رفتن داده ممیزی ۱، پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱، عملیات کنترل دسترسی، حفاظت کامل از اطلاعات باقیمانده در منابع ، ورود داده‌های کاربری به محصول با مشخصه امنیتی، صحت داده‌های کاربری ذخیره شده ۲، مدیریت احراز هویت ناموفق، تعریف مشخصات کاربر، مدیریت کلمه عبور، احراز هویت کاربر، سازوکار احرازهویت چندگانه، شناسایی کاربر، انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر، مدیریت مشـخصـه‌های امنیتی، مقداردهی اولیه مشـخصـه‌ها، مدیریت داده‌های محصـول مدیر سـیسـتم، مدیریت داده های محصول کاربرعادی، وارد کننده داده، نقش‌های امنیتی، محدودیت بر روی چندین نشست همزمان، برقراری نشست، خاتمه دادن به نشست‌ها می‌باشد. (FMT_SMF.1.1)

می‌توان در هر یک از ماژول‌های سـیسـتم نقش‌های مورد نیاز را تعریف نمود. سـیسـتم می‌تواند کاربران را با نقش‌های مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت‌های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود کند. (FMT_SMR.1.1, FMT_SMR.1.2)

محصـول می‌تواند دسـترسـی بر اسـاس نوع کاربری که بر اسـاس نقش‌های کاربر مشـخص می‌شـود را بر روی عملیات‌های مانند ایجاد، تغییر، ویرایش و حذف موجودیت‌های فعال و غیرفعال اعمال نماید. (FMT_MOF.1.1, FMT_MSA.1.1)

محصـــول می‌تواند توانایی تغییر پیش‌فرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده‌های ممیزی و داده‌های احراز هویت را به مدیر سیستم و توانایی تغییر پیش‌فرض، پرس و جو، تغییر پسورد به کاربر عادی محدود نماید. در فرایند تغییر پســورد توســط کاربر، پســورد جدید نمی‌تواند با پســورد قبلی یکســان باشــد (FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2).

۶-۶- کلاس حفاظت از توابع امنیتی هدف ارزیابی

در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می‌بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می‌نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند. (FPT_FLS.1.1)

اشتراک‌گذاری داده‌های امنیتی بین محصول و دیگر محصولات امن IT از طریق مکانیسم احراز هویت مرکزی با استفاده از روش‌هایی نظیر Directory Active و احراز هویت مرکزی CAS در سازمان مشتری انجام می‌گیرد. (FPT_TDC.1.1, FPT_TDC.1.2)

محصول می‌تواند هنگام انتقال داده‌ها بین بخش‌های مجزای خود، از آن‌ها در برابر افشاء یا تغییر محافظت نماید. محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می‌باشد. (FPT_ITT.1.1)

محصول می‌تواند مهرزمان‌های قابل اطمینانی ایجاد کند (FPT_STM.1.1).

محصول این امکان را دارد که به صورت دستی توسط پشتیبان سیستم به روزرسانی شود. این امکان با انتقال فایل بیلد شده‌ی نرم افزار به صورت امن به سرور مشتری و اجرای دستور آپدیت سیستم قابل انجام است. انتقال فایل با استفاده از پروتکل امن SFTP یا به صورت دستی با رعایت ضوابط امنیتی انجام می‌شود. (FPT_TUD_EXT.1.2)

۶-۷- کلاس تخصیص منابع

محصول از عملکرد کارکردهای اصلی سامانه در زمان بروز شکست نرم‌افزاری اطمینان حاصل می‌نماید (FRU_FLT.1.1).

۶-۸- کلاس دسترسی به هدف ارزیابی

محصول می‌تواند محدودیت تعداد نشست‌های همزمان یک کاربر را به دو صورتِ کلی (محدودیت پیش‌فرض برای سامانه، صفر به معنای بی نهایت است) و مختص یک کاربر (محدودیت برای یک کاربر، صفر به معنای بی‌نهایت است) اعمال نماید (FTA_MCS.1.1, FTA_MCS.1.2).

محصول می‌تواند کلیه نشست‌های 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.(FTA_SSL.3.1, FTA_SSL.4.1)

در صورت برقراری نشست به طور موفقیت‌آمیز، محصول قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست برا ساس روز، زمان و IP می‌باشد. توابع امنیتی هدف ارزیابی می‌تواند تاریخ، زمان، متد، مکان آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش‌های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد. توابع

امنیتی هدف ارزیابی اطلاعات تاریخچه دسترسی را از واسط کاربری پاک نمی‌نماید، بدون این‌که به کاربر فرصتی داده شود تا اطلاعات را بازبینی نماید. (FTA_TAH.1.3, FTA_TAH.1.1, FTA_TAH.1.2)

توابع امنیتی هدف ارزیابی می‌توانند از برقراری نشست براساس مکان، شماره پورت، تعداد تلاش‌های ناموفق احرازهویت، شناسه کاربر (نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی (به صورت دقیقه و بیشتر از یک دقیقه)، محدوده IP ممانعت نمایند. (FTA_TSE.1.1)

۹-۶- کلاس کانال‌ها و مسیرهای مورد اعتماد

محصول، می‌تواند مسیر ارتباطی امنی را با استفاده از پروتکل HTTPS و TLS، میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احراز هویت که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می‌تواند اجازه داشته باشد به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند و تمامی بخش‌های سیستم سازگاری کامل با پروتکل‌های امن SSL و غیره را دارند. (FTP_TRP.1.2, FTP_TRP.1.3, FTP_ITC.1.1, FTP_ITC.1.2 FTP_TRP.1.1,)

محصول می‌تواند ارتباطات را از طریق کانال امن، برای اتصال به Ldap و Active Directory راه‌اندازی نماید. (FTP_ITC.1.3)

۱۰-۶- الزامات کلاس پشتیبانی از رمزنگاری

محصول کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد طرح RSA با اندازه کلید 2048 بیت یا بیشتر تولید می‌کند و با استفاده از کتابخانه Shred که بر اساس استاندارد می‌باشد، کلیدهای رمزنگاری را از بین می‌برد. محصول رمزنگاری و رمزگشایی را مطابق با الگوریتم رمزنگاری متقارن AES- XTS و AES-CBC و AES-CCM را با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی انجام می‌دهد. (FCS_CKM.4.1, FCS_CKM.1.1 (, FCS_COP.1.1(4), FCS_COP.1.1(۳),

محصول پروتکل HTTPS را مطابق با RFC 2818 و با استفاده از TLS اجرا می‌کند و اگر گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول اتصال را برقرار نمی‌نماید. (FCS_HTTPS_EXT.1.1, FCS_HTTPS_EXT.1.1 FCS_COP.1.1, FCS_HTTPS_EXT.1.2, (۳), FCS_HTTPS_EXT.1.1,FCS_CKM.4.1, FCS_HTTPS_EXT.1.3)

محصول (RFC 5246) TLS 1.2 را پیاده سازی می‌کند و دیگر نسخه‌های TLS و SSL را رد می‌نماید. همچنین TLS با پشتیبانی از مجموعه های رمز TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 را پیاده سازی می‌نماید. همچنین محصول مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC

6125، تأیید می‌نماید. محصول کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار می‌سازد. اگر گواهی نامه سرور غیرمعتبر به نظر رسید، محصول ارتباط را برقرار نمی‌سازد. (FCS_TLSC_EXT.1.1 FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.1.3, FCS_TLSC_EXT.1.4)

محصول [TLS 1.2 (RFC5246)] را با پشتیبانی از مجموعه رمز [TLS_DHE_RSA_WITH_AES_256_CBC_SHA] مطابق با [RFC 3268] پیاده‌سازی می‌نماید: همچنین اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [TLS1.2] دارند، را رد می‌نماید. محصول پارامتر های ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت ایجاد می‌نماید. (FCS_TLSS_EXT.1.1, FCS_TLSS_EXT.1.2, FCS_TLSS_EXT.1.3)

محصول احرازهویت دوطرفه کلاینت‌های TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی می‌نماید و کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار می‌سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول ارتباط را برقرار نمی‌سازد و برای برقراری ارتباط درخواست مجوز می‌دهد و در صورت مطابقت نداشتن؛ نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه که از شناساننده کلاینت انتظار بوده است، کانال امن را برقرار نمی‌سازد. (FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5, FCS_TLSS_EXT.2.6)

۱۱-۶- الزامات شناسایی و احراز هویت

محصول مورد ارزیابی گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید می‌کند:

- تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.
- محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.
- محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [هیچ روش فسخی] تأیید کند.
- محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند:
  - گواهی‌نامه‌های موردا ستفاده برای تأیید به‌روزر سانی‌های امن و اعتبار سنجی 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.

- گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.
- گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
- گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های 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. (FIA_X509_EXT.1.1/Rev)

محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد. همچنین محصول مورد ارزیابی جهت پشتیبانی احرازهویت برای [TLS, HTTPS] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند. در صورتی محصول قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی به مدیر سیستم این امکان را می‌دهد که در زمینه‌ی پذیرش گواهی تصمیم‌گیری نماید. (FIA_X509_EXT.1.2/Rev, FIA_X509_EXT.2.1, FIA_X509_EXT.2.2)