به نام خدا

سند هدف امنیتی

سامانه اطلاعات درمان سوء مصرف مواد ایران-

IDATIS

نسخه ۵,۴,۰

شرکت بهپرداز جهان

بهمن ۱۴۰۰

نسخه ۱,۰

فهرست

۱- معرفی سند هدف امنیتی ۴
۱-۱- مرجع سند هدف امنیتی ۴
۱-۲- مرجع هدف ارزیابی ۴
۱-۳- مرور کلی هدف ارزیابی ۴
1-3-1- توابع امنیتی اصلی هدف ارزیابی ۴
۱-۳-۲- نوع هدف ارزیابی ۴
۱-۳-۳- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی ۴
۱-۴- توصیف هدف ارزیابی ۵
۱-۴-۱- حوزه فیزیکی ۵
۱-۴-۲- حوزه منطقی ۶
۲-۱- انطباق با استاندارد ارزیابی امنیتی معیار مشترک ۷
۲-۲- انطباق با پروفایل حفاظتی ۷
۲-۳- انطباق با سطح تضمین امنیتی ۷
۳- تعریف مسائل امنیتی ۸
۳-۱- مسائل امنیتی براساس پروفایل حفاظتی برنامه کاربردی تحت شبکه ۸
۳-۱-۱- تهدیدات ۸
۳-۱-۲- فرضیات ۹
۳-۱-۳- خطمشی ۱۰
۴- اهداف امنیتی ۱۱
۴-۱- اهداف امنیتی بر اساس پروفایل حفاظتی تحت شبکه ۱۱
۴-۱-۱- اهداف امنیتی برای هدف ارزیابی ۱۱
۴-۱-۲- اهداف امنیتی برای محیط عملیاتی ۱۲
۵- نیازمندی‌های امنیتی ۱۴
۵-۱- الزامات کارکرد امنیتی بر اساس پروفایل حفاظتی تحت شبکه ۱۴

۵-۱-۱- کلاس ممیزی امنیت ۱۸
۵-۱-۲- کلاس پشتیبانی از رمزنگاری ۲۱
۵-۱-۳- کلاس شناسایی و احرازهویت ۲۴
۵-۱-۴- کلاس حفاظت از داده کاربری ۲۸
۵-۱-۱- کلاس مدیریت امنیت ۳۲
۵-۱-۲- کلاس حفاظت از توابع امنیتی هدف ارزیابی ۳۶
۵-۱-۳- کلاس تخصیص منابع ۳۷
۵-۱-۴- کلاس دسترسی به هدف ارزیابی ۳۸
۵-۱-۵- کلاس کانال‌ها و مسیرهای مورد اعتماد ۳۸
۵-۲- الزامات تضمین امنیتی براساس پروفایل حفاظتی تحت شبکه ۴۰
۶- خلاصه مشخصات هدف ارزیابی ۴۱
۷- توجیهات ۴۷

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه اطلاعات درمان سوء مصرف مواد ایران- IDATIS
نسخه	۱,۰
تاریخ	بهمن ۱۴۰۰
نویسندگان	شرکت بهپرداز جهان

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت بهپرداز جهان
نام محصول	سامانه اطلاعات درمان سوء مصرف مواد ایران- IDATIS
نوع محصول	برنامه کاربردی تحت شبکه
نسخه	۵,۴,۰

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

۱- ثبت رویدادهای امنیتی

۲- ذخیره پسوردها در پایگاه داده با بهره‌گیری از الگوریتم‌های استاندارد

۳- مدیریت نقش ها

۴- احراز هویت کاربران مبتنی بر شناسه‌ی کاربری و پسورد جهت دستیابی به بخش‌های داخلی برنامه‌های کاربردی

۵- امکان انجام تنظیمات امنیتی

۱-۳-۲- نوع هدف ارزیابی

برنامه کاربردی تحت وب

۱-۳-۳- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

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

کامپوننت های محیط عملیاتی	حداقل الزامات

مرورگر	Internet Explorer- Google Chrome
سیستم عامل	CentOS Linux release 7 Oracle Redhat 7
وب سرور	Apache Tomcat 8.5.23
پایگاه داده	Oracle 12c
CPU	16 core
RAM	16 GB
HDD	200 GB

۴-۱- توصیف هدف ارزیابی

معاونت درمان وزارت بهداشت، درمان و آموزش پزشکی به منظور مدیریت فرآیند درمان نگه دارنده در مراکز درمان سوء مصرف مواد اقدام به تهیه و تولید نرم افزار IDATIS نموده است. طبق تعریف ارائه شده در پروتکل MMT درمان نگه دارنده عبارت است از:

«جایگزینی قانونی مصرف مواد مخدر غیرمجاز و غیرقانونی مراجع، با یک ماده مخدر (آگونیست) غیرتزریقی ارزان قیمت، خالص و بهداشتی با اثر بطئی و ملایم در دوز مطلوب و بهینه توسط گروه درمانگران در محیط سالم درمانی بمنظور درمان فرد، همزمان با ارائه سایر مداخلات درمانی و ثبت و پایش دقیق پیشرفت و بهبودی»

بر این اساس فرآیند تهیه شده در سامانه idatis مبتنی بر مراجعه بیمار، تهیه برنامه درمان دارویی و غیر دارویی، ارائه دوز مناسب داروی مخدر غیر تزریقی مجاز است و همچنین ارائه خدمات درمان غیر دارویی به مراجع است.

مبتنی بر هدف اصلی بالا دو هدف فرعی دیگر در این سامانه دنبال می شود:

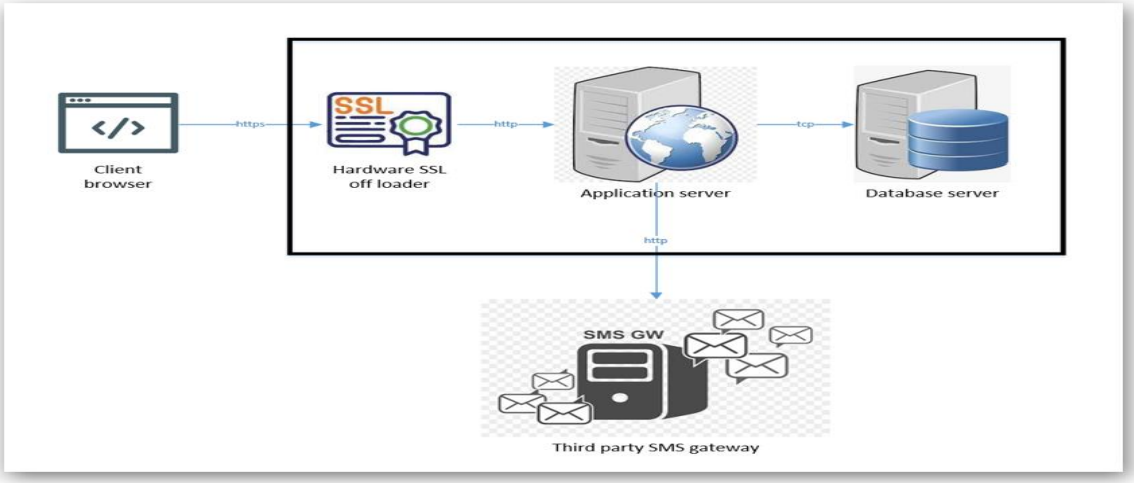
- عدم تکرار در دریافت دارو توسط شخص : که به این منظور می بایست تکراری بودن مراجع مشخص شود. لیکن مبتنی بر اصل حفظ راز داری نمی بایست به هیچ عنوان هویت شخص بیمار از اطلاعات موجود در سامانه قابل بازیابی باشد.
- رهگیری داروی مخدر : که به این منظور طبق ضوابط تعیین شده در سازمان غذا و دارو می بایست داروی مخدر به همراه کد بچ و کد رهگیری دارو در فرآیند تهیه و ارائه دارو قابل رهگیری باشد.

۴-۱-۱- حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
سامانه اطلاعات درمان سوء مصرف مواد ایران- IDATIS	۵,۴,۰

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



۲-۴-۱- حوزه منطقی

کارکردها	توصیف
ممیزی	تمامی رویدادهای قابل ممیزی شامل: تمامی ورود و خروج‌های موفق و ناموفق، تمامی تغییرات توسط کاربر در برنامه کاربردی بر روی موجودیت‌های فعال و غیرفعال، تمامی تلاش‌های موفق و غیر موفق برای خروج اطلاعات، رویدادهای مرتبط با محدودیت نشست‌های همزمان، رویدادهای مرتبط با منقضی شدن (session timeout) نشست‌های بیکار، تمامی شکست‌هایی که ممکن است در محصول ناشی از تلاش برای انجام عملیات غیرمجاز اتفاق بیفتد، ثبت می‌شود.
رمزنگاری	از الگوریتم درهم‌سازی SHA256 استفاده شده است.
حفاظت از داده کاربری	دسترسی‌های موجودیت‌های فعال بر روی موجودیت‌های غیرفعال از طریق انجام عملیات‌های مختلف در هدف ارزیابی، به طور مشخص تعریف شده و در صورتی که عملیاتی خارج از دسترسی‌های تعریف شده باشد، به عنوان عملیات غیرمجاز محسوب شده و علاوه بر اینکه اجازه انجام آن داده نمی‌شود، لاگ آن نیز ثبت می‌گردد.
شناسایی و احرازهویت	به منظور شناسایی و احرازهویت از دو روش استفاده می‌شود: ۱- ارسال OTP از طریق تلفن همراه ۲- از طریق وارد کردن نام کاربری و رمزعبور
مدیریت امنیت	مجوز تغییر پیکربندی کارکردهای محصول فقط در اختیار مدیر سیستم بوده و سایر کاربران غیرمجاز قادر به انجام این تغییرات نمی‌باشند.
حفاظت از توابع امنیتی محصول	در زمان رخدادهای انواع شکست‌های نرم‌افزاری و سخت‌افزاری، محصول وضعیت امن را حفظ نماید.
تخصیص منابع	تمامی شکست‌های نرم‌افزاری که ممکن است در محصول ناشی از تلاش برای انجام عملیات غیرمجاز با دسترسی غیرمجاز و ... اتفاق بیفتد، ثبت می‌شود.
دسترسی به محصول	پالیسی های امنیتی در رابطه با نشست‌های برقرارشده با محصول لحاظ گردیده

کارکردها	توصیف
	است.
کانال‌ها/ مسیرهای مورداعتماد	جهت جلوگیری از شنود و گم شدن داده‌ها در هنگام انتقال، از پروتکل https به همراه گواهینامه معتبر برای انتقال داده بین کاربر و سرور استفاده می‌شود.

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 5,2017
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	برنامه های 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- مسائل امنیتی براساس پروفایل حفاظتی برنامه کاربردی تحت شبکه

۳-۱-۱- تهدیدات

تهدید	توصیف
T.UNAUTHORIZED_ACCESS	مهاجم میتواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا کند. این دسترسی میتواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد .مهاجم میتواند با سود بردن از نقضهای امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری آزمون بر روی سیستم واقعی به محصول دسترسی پیدا کند. 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، واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم میتواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر دادههای حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها و مستندات تضمین شده نیست. مهاجم ممکن است درصدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا کند.
T.REPUDIATION	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول میتواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول است تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم میتواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم میتواند با اضافه کردن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه کند.
T.DATA_DISCLOSURE	داده های محرمانه که توسط محصول محافظت میشوند میتواند بدون مجوز افشاء گردد. برای مثال،کاربر عادی میتواند به یک رکورد،سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی میتواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور واردکننده داده میتواند

تهدید	توصیف
	عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
T.DENIAL_OF_SERVICE	مهاجم میتواند سبب گردد محصول در یک بازه زمانی غیرقابل دسترسی یا بلا استفاده گردد. این امر معمولا با ارسال درخواستهای بسیار در یک بازه زمانی کوتاه صورت میگیرد طوری که محصول قادر به پاسخ نخواهد بود .نوع ساده ای از حمله شامل ارسال درخواستهای بسیار از یک رنج IP مشخص است که به نام حمله DoS شناخته میشود. نوع دیگر پیشرفته تر حمله DDoS است که از BOTNET استفاده میکند و محدودیتی بر روی آدرس IP ورودی ندارد.
T.HARMFUL_DATA	مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول وارد کند. با استفاده از این تهدید، مهاجم میتواند به داده کاربر خاص دسترسی پیدا کند، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
T.ELEVATION_OF_PRIVILEGES	مهاجم میتواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر کند.
T.NETWORK_EAVESDROP	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر میشود تا انتقال داده های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده های ردوبدل 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 میکند.

۲-۱-۳- فرضیات

فرضیه	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 داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب-پذیری‌های شناخته شده را اتخاذ می‌نمایند.
A.SECURE_ENVIRONMENT	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای

فرضیه	توصیف
	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 DoSو شنود شبکه و غیره حفاظت می‌شوند .
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.
A.DIST_DENIAL_OF_SERVICE	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می¬شود.

۳-۱-۳- 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، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می-نمایند. این خط‌مشی سازمانی بسیار مهم است به خصوص زمانیکه

خطمشی	توصیف
	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.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی بر اساس پروفایل حفاظتی تحت شبکه

۴-۱-۱- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
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.
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.
O.DATA_FLOW_CONTROL	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده-های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف شده می‌تواند بیانگر حمله DoS

هدف امنیتی	توصیف
	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.
O.DATA_INTEGRITY	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
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.
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.
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.

۲-۱-۴- 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

هدف امنیتی	توصیف
	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 مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می-گیرد.
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 می-باشد. 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 بر اساس پروفایل حفاظتی تحت شبکه

در الزامات کارکردی زیر عملیات انتخاب [درون براکت و به صورت underlined]و عملیات اختصاص [**درون براکت و با استایل bold**] نمایش داده خواهند شد.

شماره مؤلفه	نام کلاس	نام الزام
۱	**FAU: ممیزی امنیت**	**FAU_GEN.1**: تولید داده ممیزی
۲		
۳		**FAU_GEN.2**: مرتبط نمودن هویت کاربر به رویداد
۴		**FAU_SAR.1**: بازبینی داده ممیزی
۵		
۶		**FAU_SAR.2**: بازبینی داده ممیزی محدود
۷		**FAU_SAR.3**: بازبینی داده ممیزی قابل انتخاب
۸		**FAU_SEL.1**: انتخاب داده ممیزی
۹		**FAU_STG.1**: ذخیره سازی رویدادهای ممیزی
۱۰		
۱۱		**FAU_STG.3**: اقدامات لازم در زمان از دست رفتن داده ممیزی
۱۲		**FAU_STG.4**: پیشگیری از اتلاف و از بین رفتن داده ممیزی
۱۳	**FCS:عملیات رمزنگاری**	**FCS_COP.1(1)**: عملیات رمزنگاری(۱)
۱۴		**FCS_COP.1(2)**: عملیات رمزنگاری(۲)
۱۵		**FCS_TLSC_EXT.1**: الزامات پروتکل TLS Client ۱
۱۶		
۱۷		
۱۸		**FCS_TLSC_EXT.4**: الزامات پروتکل TLS Client ۴
۱۹		**FCS_TLSS_EXT.1**: الزامات پروتکلTLS Server
۲۰		
۲۱		
۲۲	**FDP:حفاظت از داده کاربری**	**FDP_ACC.1**: خط مشی کنترل دسترسی
۲۳		**FDP_ACF.1**: عملیات کنترل دسترسی

۲۴		
۲۵		
۲۶		
۲۷		**FDP_RIP.2**: حفاظت کامل از اطلاعات باقیمانده در منابع
۲۸		**FDP_ITC.2**: ورود داده کاربری به محصول با مشخصه امنیتی
۲۹		
۳۰		
۳۱		
۳۲		
۳۳		**FDP_ETC.2**: خروج داده کاربری از محصول با مشخصه امنیتی
۳۴		
۳۵		
۳۶		
۳۷		**FDP_SDI.1**: صحت داده کاربری ذخیره شده
۳۸		
۳۹	**FIA:شناسایی و احراز هویت**	**FIA_AFL.1**: مدیریت احرازهویت ناموفق
۴۰		
۴۱		**FIA_ATD.1**: تعریف مشخصات کاربر
۴۲		**FIA_PMG_EXT.1**: مدیریت کلمه عبور
۴۳		**FIA_UAU.2**: احراز هویت قبل از هر اقدام
۴۴		**FIA_UID.2**: شناسایی قبل از هر اقدام
۴۵		**FIA_UAU.5**: سازوکار احرازهویت چندگانه
۴۶		
۴۷		**FIA_USB.1**: انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر
۴۸		
۴۹		
۵۰		**FIA_X509_EXT.1**: اعتبارسنجی گواهی x509
۵۱		
۵۲		**FIA_X509_EXT.2**: احراز هویت از طریق گواهی X509
۵۳		
۵۴	**FMT:مدیریت امنیت**	**FMT_MOF.1**: مدیریت کارکرد در محصول
۵۵		**FMT_MSA.1**: مدیریت مشخصه های امنیتی

۵۶		**FMT_MSA.3**: مقداردهی ایستای مشخصه های امنیتی
۵۷		
۵۸		**FMT_MTD.1(1)**: مدیریت داده‌های توابع امنیتی هدف ارزیابی (مدیر سیستم)
۵۹		**FMT_MTD.1(2)**: مدیریت داده‌های توابع امنیتی هدف ارزیابی (کاربر عادی، وارد کننده داده)
۶۰		**FMT_SMF.1**: کارکردهای مدیریتی محصول
۶۱		**FMT_SMR.1**: نقشهای امنیتی
۶۲		
۶۳	**FPT:حفاظت از داده توابع امنیتی هدف ارزیابی**	**FPT_FLS.1**: حفظ وضعیت امن در زمان شکست
۶۴		**FPT_ITT.1**: انتقال داده امنیتی در داخل محصول
۶۵		**FPT_TDC.1.2**: سازگاری داده امنیتی بین محصول و موجودیت امن
۶۶		
۶۷		**FPT_STM.1**: مهرهای زمانی
۶۸		**FPT_TUD_EXT.1**: به روزرسانی امن
۶۹		
۷۰	**FRU:تخصیص منابع**	**FRU_FLT.1**: تحمل خطا
۷۱	**FTA:دسترسی به هدف ارزیابی**	**FTA_MCS.1**: محدودیت بر روی چندین نشست همزمان
۷۲		
۷۳		**FTA_SSL.3**: خاتمه دادن به نشستها توسط محصول
۷۴		**FTA_SSL.4**: خاتمه دادن به نشستها توسط کاربر
۷۵		**FTA_TAH.1**: سوابق دسترسی به محصول
۷۶		
۷۷		
۷۸		**FTA_TSE.1**: برقراری نشست
۷۹	**FTP:کانال‌ها و مسیرهای امن**	**FTP_TRP.1**: مسیر امن
۸۰		
۸۱		
۸۲		**FTP_ITC.1**: کانال امن
۸۳		
۸۴		

۸۵	**سایر الزامات مبتنی بر انتخاب**	عملیات رمزنگاری -۱رمزنگاری و رمزگشایی ۱ (۳)
۸۶		الزامات پروتکل**TLS Server**/ احرازهویت (۴)
۸۷		الزامات پروتکل**TLS Server**/ احرازهویت (۵)
۸۸		الزامات پروتکل**TLS Server**/ احرازهویت (۶)

۱-۱-۵- کلاس ممیزی امنیت

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
FAU_GEN.1	FPT_STM.1	۱	**FAU_GEN.1.1**	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.
		۲	**FAU_GEN.1.2**	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 • هیچ اطلاعات دیگری
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.
FAU_SAR.1	FAU_GEN.1	۴	**FAU_SAR.1.1**	بازبینی داده ممیزی ۱: محصول باید امکان خواندن **[کلیه داده‌های ممیزی]** از کل رکوردهای ممیزی را برای **[مدیر سیستم]** فراهم نماید.
		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**	محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.
FAU_SAR.3	FAU_SAR.1	۷	**FAU_SAR.3.1**	بازبینی داده ممیزی قابل انتخاب ۱: محصول باید امکان انجام **[متدهای انتخاب و مرتب‌سازی]** رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس **[حساب کاربری، تاریخ/زمان، مکان، روش اتصال کاربر، درجه اهمیت رکوردها، نوع رخداد]** مرتب نماید.
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	۸	**FAU_SEL.1.1**	محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید:

			• [نوع رخداد] • **[هیچ معیار دیگری]**	
FAU_STG.1	FAU_GEN.1	۹	**FAU_STG.1.1**	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید.
		۱۰	**FAU_STG.1.2**	محصول باید قادر به **[تشخیص]** تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد.
FAU_STG.3	FAU_STG.1	۱۱	**FAU_STG.3.1**	محصول در صورت تجاوز دنباله ممیزی از **[یک محدودیت از پیش تعریف شده]** باید **[با استفاده از ارسال پیام کوتاه کاربران مربوطه را مطلع نماید.]**
FAU_STG.4	FAU_STG.1	۱۲	**FAU_STG.4.1**	محصول در صورت پر شدن دنباله ممیزی، باید [روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید] و **[هیچ اقدام دیگری]**.

جدول۱- لیست رویدادهای قابل ممیزی

مؤلفه	رویداد قابل ممیزی	جزئیات
FAU_SAR.2	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
FAU_SAR.1	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
FAU_SEL.1	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی‌که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
FAU_STG.3	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
FAU_STG.4	عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
FDP_SDI.2	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی	

	(پایه)	
FIA_UAU.1	ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
FIA_UAU.5	ثبت نتایج احرازهویت (حداقل) ثبت هر سازو کار احرازهویت فعال همراه با نتیجه نهائی (پایه)	
FIA_UID.1	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال
FIA_PMG_EXT.1	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
FIA_USB.1	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)	
FMT_MSA.1	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	
FMT_MTD.1(1)	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
FMT_MTD.1(2)	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
FCS_COP.1(1)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
FCS_COP.1(2)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
FDP_ACF.1	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول	شناسایی داده‌های موجودیت غیرفعال

	(حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	
FDP_ITC.2	ورود داده کاربری موفقیت آمیز، شامل هر گونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	
FDP_ETC.2	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	
FMT_MOF.1	تمامی تغییرات در رفتارهای کارکردی محصول	
FMT_SMF.1	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
FMT_SMR.1	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش می‌باشد (حداقل)	
FPT_TDC.1.2	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	
FPT_FLS.1	ثبت شکست در محصول (پایه)	
FRU_FLT.1	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست می‌باشد (پایه)	
FTA_TSE.1	ثبت منع آغاز نشست بدلیل مکانیزم آغاز نشست (حداقل) ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه)	
FTA_MCS.1	ثبت رد یک نشست مبتنی بر محدودیت نشست‌های همزمان (حداقل)	
FTA_SSL.3 **FTA_SSL.4**	ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	

۲-۱-۵- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.1(1)	FDP_ITC.1 FDP_ITC.2 FCS_CKM.1	۱	**FCS_COP.1.1(1)**	محصول باید **[برای وارسی صحت داده‌های ممیزی و داده‌های رکورد]** بر اساس یک الگوریتم رمزنگاری مشخص **[SHA256]** و اندازه کلید رمزنگاری **[هیچ کلید]** اجرا شود که مطابق با **[FIPS 180-3]** باشد.
FCS_COP.1(2)	FDP_ITC.1 FDP_ITC.2 FCS_CKM.1	۲	**FCS_COP.1.1(2)**	محصول باید **[تولید داده درهم‌سازی]** بر اساس یک الگوریتم رمزنگاری مشخص **[SHA256]**و اندازه-کلید رمزنگاری **[هیچ کلید]** اجرا شود که مطابق با **[FIPS 180-3]** باشد.
FCS_TLSC_EXT.1	-	۳	**FCS_TLSC_EXT.1.1**	محصول باید [TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] 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_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				]
		۴	**FCS_TLSC_EXT.1.2**	محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.
		۵	**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]
FCS_TLSC_EXT.4	-	۶	**FCS_TLSC_EXT.4.1**	محصول بایـد در پیـام Client Hello [Supported Elliptic Curves Extension را بـه همـراه NIST curve های [secp256r1, secp384r1 secp521r1] و هیچ منحنی دیگری ارائه کند.]

۳-۱-۵- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
FIA_AFL.1	FIA_UAU.1	۱	**FIA_AFL.1.1**	محصول باید بتواند با استفاده از [یک عدد مثبت قابل تنظیم توسط مدیر **[بین صفر تا ۹۹۹]**]، تلاش‌های ناموفق احرازهویت مرتبط با **[ورود به سیستم]** را تشخیص دهد.
		۲	**FIA_AFL.1.2**	زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [بیشتر از حد تعیین شده رسید]، محصول باید **[بلاک کردن کاربر]** را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.
FIA_ATD.1	-	۳	**FIA_ATD.1.1**	محصول باید مشخصه‌های 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)** • **[اطلاعات زمانی آخرین دسترسی]**
FIA_PMG_EXT.1	-	۴	**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: • کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: ["@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" **, [هیچ کاراکتر دیگری]]**] باشد. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.
FIA_UAU.1	-	۵	**FIA_UAU.1.1**	محصول باید پیش از احرازهویت کاربر، اجازه اقدامات میانی زیر را به کاربر دهد: [بازیابی کلمه عبور ،] • **دانلود اسناد** • **ثبت مرکز درمانی**

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
				• **ویرایش مرکز درمانی** • **سوالات متداول** • **هیچ اقدام دیگری**]]
FIA_UAU.1	-	۶	**FIA_UAU.1.2**	محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت نماید.
FIA_UAU.5	-	۷	**FIA_UAU.5.1**	سازوکار احرازهویت چندگانه ۱: محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد: **]** • **نام کاربری و کلمه عبور** • **ارسال OTP از طریق ارسال پیام کوتاه به تلفن همراه** **[**
		۸	**FIA_UAU.5.2**	محصول باید هر کاربر متقاضی احرازهویت را مطابق قوانین ذیل احرازهویت نماید: **]** • **کاربران از راه‌دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احرازهویت چندگانه (مانند Dual factor authentication) استفاده کند.** • **[هیچ قانون دیگری]**
FIA_UID.1	-	۹	**FIA_UID.1.1**	محصول پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم می‌آورد:] • **دانلود اسناد** • **ثبت مرکز درمانی** • **ویرایش مرکز درمانی** • **سوالات متداول** **هیچ اقدام دیگری** [
FIA_UID.1	-	۱۰	**FIA_UID.1.2**	توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
				داشته باشد، با موفقیت شناسایی نماید.
FIA_USB.1	FIA_ATD.1	۱۱	**FIA_USB.1.1**	محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: **[** • **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)** • **[هیچ مشخصه دیگری]** **]**
		۱۲	**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: **[** • **زمانی‌که یک نشست جدید برقرار می‌شود، اعتبار نشست‌های قبلی باید از بین برود (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد.** • **اطلاعات پیشینه احراز هویت باید بروزرسانی گردد.** • **[هیچ قانون دیگری]** **]**
		۱۳	**FIA_USB.1.3**	محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: **[** • **هیچ تغییری در طول نشست فعال مجاز نمی‌باشد،** • **[هیچ قانون دیگری]** **]**
FIA_X509_EXT.1	-	۱۴	**FIA_X509_EXT.1.1**	محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند:

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
				• 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 [لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵] 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. ○ 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

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
				extendedKeyUsage خود داشته باشند.
		۱۵	**FIA_X509_EXT.1.2**	محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.
FIA_X509_EXT.2	-	۱۶	**FIA_X509_EXT.2.1**	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای [TLS]، و [**ارسال OTP احراز هویت**] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.
		۱۷	**FIA_X509_EXT.2.2**	در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید[گواهی را نپذیرد.]

۴-۱-۵- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1	FDP_ACF.1	۱	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید: **]** • **موجودیت فعال:** **[مدیر سیستم، کاربر عادی، [ممیز، پرستار، مسئول فنی، کاربر دانشگاه علوم پزشکی، کاربر وزارت بهداشت، کاربر ستاد مبارزه با مواد مخدر، درمانگر، کاربر معاونت غذا و دارو، پشتیبان سیستم، موسس مرکز درمانی، کاربر فرم کاهش آسیب، ارزیابی الکل]]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **موجودیت غیرفعال:** **رکوردها، مستندات و فرا-داده**[1] **داده متعلق به کاربران** **داده احرازهویت** **داده با این معیارها: [هیچ معیار دیگری]** **[هیچ موجودیت دیگری]** • **عملیات:** **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	FDP_ACC.1 FMT_MSA.3	۲	**FDP_ACF.1.1**	محصول باید **[خط‌مشی‌های کنترل دسترسی]** را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: **]** • **هویت کاربر** • **نقش‌ها و مجوزهای کاربر مجاز** • **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند** • **[هیچ مشخصه دیگری]** **]**

[1] Metadata

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۳	**FDP_ACF.1.2**	محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید: **[** **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.** **]**
		۴	**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 رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند.** • **کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.** • **[هیچ قانون دیگری]** **]**
		۵	**FDP_ACF.1.4**	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: **[** **تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده،** **[هیچ قانون دیگری]]**
	-	۶	**FDP_RIP.2.1**	محصول باید تضمین نماید در هنگام [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.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_SDI.2	- -	۷	**FDP_SDI.2.1**	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[۲] داده‌های کاربری ذخیره شده]** پایش نماید.
		۸	**FDP_SDI.2.2**	هنگام تشخیص خطای صحت داده، محصول باید **[ثبت رکورد لاگ در برنامه]** را صورت دهد.

[۲] Hash

۱-۱-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	۱	**FMT_MOF.1.1**	محصول باید امکان [تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] توابع **[تمام کارکردهای مربوط به مدیریت محصول]** را به **[مدیر سیستم]، [هیچ نقش دیگری]]** محدود نماید
FMT_MSA.1	[FDP_ACC.1 , or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	۲	**FMT_MSA.1.1**	**محصول باید با اعمال** [خط‌مشی کنترل دسترسی]**،[امکان تغییر پیش‌فرض، پرس و جو، تغییر، حذف،** [هیچ عملیات دیگری]**] مشخصه‌های امنیتی** **]** • **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)** • **[هیچ مشخصه دیگری]** [را به [**مدیر سیستم و هر کاربری که مجوز لازم را دارد**] محدود نماید.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	۳	**FMT_MSA.3.1**	محصول برای مشخصه های امنیتی که برای اعمال [**خط مشی کنترل دسترسی**] استفاده می شوند، باید مقادیر پیش فرض محدود شده ای درنظر بگیرد.
		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.
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	۵	**FMT_MTD.1.1 (1)**	محصول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، **[هیچ کارکرد دیگری]**] [**رخدادهای ممیزی ، مجوزهای نقش و دسترسی، داده‌های احراز هویت و تنظیمات امنیتی**] را به [**مدیر سیستم**] محدود نماید.
		۶	**FMT_MTD.1.1 (2)**	محصول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [**هیچ کارکرد دیگری**]] [**تغییر رمز عبور و بازیابی رمز عبور**] را به [**کاربر عادی**] محدود نماید.

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
FMT_SMF.1	-	۷	**FMT_SMF.1.1**	محصول باید قادر به انجام [**کارکردهای مدیریتی که در جدول زیر آمده است**] باشد:

مولفه	عملیات مدیریتی
FAU_GEN.1	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
FAU_SEL.1	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
FAU_STG.3	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
FAU_STG.4	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
FDP_ACF.1	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
FDP_RIP.2	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پیکربندی باشد.
FDP_ITC.2	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
FDP_SDI.1	عملیاتی برای تشخیص یک خطای صحت داده که می-تواند قابل پیکربندی باشد.
FIA_AFL.1	مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان	
				FIA_ATD.1	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد. [اختیاری]
				FIA_PMG_EXT.1	مدیریت تنظیمات و الزامات و قابلیت‌ها برای تنظیم کلمه عبورها
				FIA_UAU.1	مدیریت داده‌های احرازهویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احرازهویت کاربر انجام می‌شوند.
				FIA_UAU.5	مدیریت سازوکارهای احرازهویت مدیریت قوانین مرتبط با احرازهویت
				FIA_UID.1	مدیریت شناسایی کاربران]اختیاری[مدیریت تغییرات و فرایندهایی مانند(ادرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.
				FIA_USB.1	مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و تغییر دهد.
				FMT_MSA.1	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
				FMT_MSA.3	مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
				FMT_MTD.1	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
				FMT_MTD.1(2)	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
				FMT_SMR.1 مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند. **FTA_MCS.1** مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر **FTA_TSE.1** مدیریت شرایط آغاز نشست توسط مدیر مجاز **FTA_SSL.3** 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	۸	**FMT_SMR.1.1**	نقش‌های زیر در محصول باید تعریف شده باشد: ○ [مدیر سیستم[**کاربر دانشگاه علوم پزشکی ، کاربر معاونت غذا و دارو ، کاربر وزارت بهداشت ، کاربر سازمان غذا و دارو ، پشتیبان سیستم، روانشناس، پزشک-مسئول فنی، پرستار، درمانگر، مددکار، موسس مرکز درمانی، ارزیابی الکل، کاربر فرم کاهش آسیب، کاربرمبارزه با ستاد مبارزه با مواد مخدر، ممیز**]]
		۹	**FMT_SMR.1.2**	محصول، باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند.

۲-۱-۵- کلاس حفاظت از توابع امنیتی هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.1.1	-	۱	**FPT_FLS.1.1**	محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: **[شکست‌های نرم‌افزاری، شکست‌های سخت‌افزاری]**
FPT_ITT.1	FTP_TRP.1.1	۲	**FPT_ITT.1.1**	محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که باهم ارتباط دارند، محافظت نماید.
FPT_TDC.1	FTP_TRP.1.1	۳	**FPT_TDC.1.1**	محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [**داده های امنیتی لیست شده در زیر**] را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. **]** **نام کاربری و کلمه عبور sender** **آدرس Sender** **پورت ارسالی** **پروتکل ارتباطی** **[**
		۴	**FPT_TDC.1.2**	محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [**از پروتکل TLS**] استفاده نماید.
FPT_STM.1	-	۵	**FPT_STM.1.1**	محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند.

۳-۱-۵- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.1	FPT_FLS.1	6	**FRU_FLT.1.1**	محصول باید از عملکرد [**تمام کارکردهای اصلی**] هنگام رویداد شکست‌های زیر اطمینان حاصل نماید: [**شکست نرم‌افزاری، [هیچ شکست دیگری]**]

۴-۱-۵- کلاس دسترسی به هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_MCS.1	FIA_UID.1	۱	**FTA_MCS.1.1**	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.
		۲	**FTA_MCS.1.2**	محصول باید به صورت پیش‌فرض، [**۲نشست همزمان**] برای هر کاربر در نظر بگیرد.
FTA_SSL.3	-	۳	**FTA_SSL.3.1**	محصول باید کلیه نشست‌های تعاملی راه‌دور[۳] را پس از مدت زمان **[بازه زمانی که توسط مدیرتنظیم می-شود]** غیرفعال بودن، خاتمه دهد.
FTA_SSL.4	-	۴	**FTA_SSL.4.1**	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.
FTA_TAH.1	-	۵	**FTA_TAH.1.1**	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست براساس [روز، زمان، **[هیچ مشخصه دیگر]**] باشد.
		۶	**FTA_TAH.1.2**	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید [تاریخ، زمان، متد، مکان] آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.
		۷	**FTA_TAH.1.3**	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	-	۸	**FTA_TSE.1.1**	توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس [**تعداد تلاش های ناموفق احرازهویت، شناسه کاربر(نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP [هیچ مشخصه دیگری]**] ممانعت نماید.

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

[۳] Remote

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.1	-	۱	FTP_TRP.1.1	محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [TLS] 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.
		۲	FTP_TRP.1.2	محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.
		۳	FTP_TRP.1.3	باید استفاده از کانال امن را برای احرازهویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی نماید.
FTP_ITC.1	-	۴	FTP_ITC.1.1	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [TLS] میان خود و موجودیت IT معتبر، [**[سرور پیام کوتاه]]** 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.
		۵	FTP_ITC.1.2	محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.
		۶	FTP_ITC.1.3	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای **[ارسال پیامک جهت احراز هویت ثانویه و هشدار به ادمین برای حدآستانه لاگ ، فراموشی رمز عبور، ارسال مشخصات مرکز درمانی ثبت شده]** راه‌اندازی نماید.

۲-۵- الزامات تضمین امنیتی براساس پروفایل حفاظتی تحت شبکه

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده مـی-شود که لیست الزامات آن در جدول زیر آمده است.

- **الزامات تضمین امنیتی براساس پروفایل حفاظتی تحت شبکه:**

نام کلاس	نام الزام	توضیحات
Development	**ADV_FSP.1**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.1**	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Life cycle Support	**ALC_CMC.1**	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول
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

۶- خلاصه مشخصات هدف ارزیابی

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 IP، تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال، نام سامانه، آدرس دامنه درخواستی و نتیجه(موفقیت یا شکست) رویداد را ثبت نماید. (FAU_GEN.1.1، FAU_GEN.1.2، FAU_GEN.2.1)
- محصول دارای قابلیت مشاهده اطلاعات ممیزی شامل ورود موفق، ورود ناموفق، قفل کاربر، ویرایش، حذف و ایجاد موجودیت‌های غیرفعال امنیتی، به شکل خوانا و قابل درک برای مدیر سیستم و کاربران مجاز می‌باشد. همچنین محصول می‌تواند از خواندن رکوردهای ممیزی توسط کاربران غیر مجاز جلوگیری کرده و تلاش‌ها برای دسترسی غیرمجاز را ثبت نماید. گزارش ممیزی امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه(موفقیت یا شکست) رویداد مرتب نماید. همچنین امکان انتخاب و مدیریت رویدادهایی که برنامه باید از آنها لاگ ثبت کند، برای ادمین فراهم شده است. (FAU_SAR.1.1، FAU_SAR.1.2، FAU_SAR.2.1، FAU_SAR.3.1، FAU_SEL.1.1)
- محصول امکان حذف غیرمجاز داده ممیزی را ندارد. محصول قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی است و مدیر سامانه را از این تغییرات مطلع می‌سازد.

جهت پیاده سازی فیلدهای مهم در نظر گرفته شده است، این فیلدها کنار هم قرار داده شده و سپس با استفاده از الگوریتم SHA256 هش ایجاد می شود و مقدار هش در یک ستون جدید در جدول رکوردهای ممیزی نگهداری می شود. سپس هر بار که واسط رویدادهای سیستم مشاهده می شود، بررسی صحت داده ها صورت می گیرد.

TBL_userTracking
Table Fields (EventName + UserName + CreateDate + Result)

رکورد لاگ دستکاری شده با رنگ قرمز مشخص می‌شود. هچنین رکورد جدیدی که نشان دهنده دستکاری داده می باشد برای اطلاع رسانی به مدیر ثبت خواهد شد.

مقدارحد آستانه رکوردهای ممیزی براساس تعداد رکوردهای ممیزی، از طریق بخش تنظیمات ممیزی توسط مدیر سامانه تنظیم می شود و رکورد لاگ تنظیمات انجام شده ثبت خواهد شد. سپس در صورت رسیدن تعداد رکوردهای جدول TBL_userTracking، به عدد تنظیمی، رکورد ممیزی با عنوان "رسیدن به حد آستانه" در بخش گزارش رخدادنگاری سامانه ثبت خواهد شد و پیامکی جهت اطلاع رسانی به مدیر سامانه (تنظیمات شماره موبایل جهت اطلاع رسانی از طریق واسط تنظیمات امنیتی) ارسال خواهد شد. همچنین در بخش تنظیمات سامانه پارامتری جهت تنظیم مدت زمان توسط مدیر سامانه با عنوان " دوره اجرای زمانبندی حذف لاگ ممیزی به دقیقه" وجود دارد که در طول این مدت زمان تنظیم شده که به مدیر فرصت می دهد، تا تعداد رکوردهای ممیزی افزایش دهد و در صورت عدم افزایش تعداد رکوردها بعد از گذشت زمان بازنویسی روی رکوردهای ممیزی قدیمی صورت می‌گیرد و رکورد لاگ مرتبط با آن ثبت خواهد شد.(FAU_STG.1.1، FAU_STG.1.2، FAU_STG.3.1، FAU_STG.4.1)

کلاس عملیات رمزنگاری

- محصول برای بررسی صحت داده‌های ممیزی و امنیتی براساس الگوریتم رمزنگاری SHA256 اطلاعات را رمزنگاری می‌نماید. طول کلید ۲۵۶ بایت می‌باشد.((FCS_COP.1.1(1) ، FCS_COP.1.1(2))
- محصول جهت برقرار ارتباط از لیست Cipher suit های مجاز پشتیبانی می نماید.(FCS_TLSC_EXT.1.1)

- محصول در صورت عدم اعتبار گواهینامه سرور خارجی، اجازه برقراری ارتباط نمی‌دهد. (FCS_TLSC_EXT.1.2 وFCS_TLSC_EXT.1.3)
- محصول از elliptic curve های secp256r1, secp384r1, secp521r1 استفاده میکند که مورد تایید استاندارد است. (FCS_TLSC_EXT.4.1)
- محصول Cipher suit های مجاز پشتیبانی می نماید. (FCS_TLSS_EXT.1.1)

کلاس شناسایی و احراز هویت

- مدیرسامانه امکان تنظیم تعداد تلاش‌های ناموفق برای احراز هویت را دارد. در صورتی که تعداد تلاش های ناموفق از تعداد تعیین شده عبور کند، حساب کاربری برای مدت زمان مشخصی که توسط مدیر سامانه قابل تنظیم است، مسدود خواهد شد. (FIA_AFL.1.1، FIA_AFL.1.2)
- محصول مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری می‌نماید. (FIA_ATD.1.1)
  - شناسه کاربر
  - داده احرازهویت (رمز عبور و نام کاربری)
  - نقش کاربر
  - وضعیت حساب کاربری (فعال، غیرفعال،مسدود)

- سازمان کاربر

- محصول امکان مدیریت پیچیدگی رمزعبور و طول آن را دارد. حداقل طول رمز عبور ۸ کاراکتر است. این امکان توسط مدیرسامانه قابل تنظیم است. به دلیل مسائل امنیتی سیاست پیچیدگی پسورد بصورت پیش فرض روی سامانه فعال است. (FIA_PMG_EXT.1.1)
- کاربران می توانند قبل از احرازهویت به لینک های زیر دسترسی داشته باشند:

– دانلود اسناد
– ثبت مرکز درمانی
– ویرایش مرکز درمانی
– سوالات متداول (FIA_UAU.1.1،FIA_UAU.1.2 ، FIA_UID.1.1 ، FIA_UID.1.2)

- سامانه امکان احراز هویت دو عاملی با نام کاربری و رمزعبور و ارسال کد امنیتی به شماره همراه کاربر را دارد. لازم به ذکر است با توجه بیزنس محصول فقط شماره موبایل مدیر سامانه (کاربر superadmin) از طریق پایگاه داده در جدول tble_telephone رکورد با id=1 قابل تنظیم می باشد. (FIA_UAU.5.1، FIA_UAU.5.2)
- محصول مشخصه‌های امنیتی کاربر فعال را نگهداری می‌نماید. محصول پیشینه احراز هویت کاربر را نگهداری می‌نماید. کاربر امکان برقراری نشست های همزمان براساس چیزی که مدیر تعیین کرده است را دارد. (FIA_USB.1.1، FIA_USB.1.2، FIA_USB.1.3)
- محصول تنها در صورت دریافت گواهی معتبر از سرور خارجی، اجازه برقراری ارتباط را می‌دهد. (FIA_X509_EXT.1.1، FIA_X509_EXT.1.2، FIA_X509_EXT.2.1 و FIA_X509_EXT.2.2)

کلاس حفاظت از داده کاربری

- محصول توانایی کنترل دسترسی و تخصیص دسترسی به اطلاعات سامانه را دارد. این امکان توسط مدیرسیستم قابل مدیریت است. مدیرسیستم امکان تعیین نقش کاربران که تعیین کننده سطح دسترسی آنها به موجودیت‌های غیرفعال است را دارد. (FDP_ACF.1.1)
- محصول اطلاعات هویت کاربر و نشست آن را جهت بررسی دسترسی کاربر و ثبت در اطلاعات ممیزی نگهداری می‌نماید و کاربران با توجه به نقش خود به اطلاعات و کارکردهای سامانه دسترسی دارند. امکان ایجاد چندین نشست همزمان در این محصول وجود دارد و مدیر سیستم می‌تواند این تعداد را تعیین کند. (FDP_ACF.1.1، FDP_ACF.1.2، FDP_ACF.1.3، FDP_ACF.1.4)
- محصول تضمین می‌نماید در زمان آزادسازی منابع اطلاعات آنها به طور کامل حذف خواهد گردید. (FDP_RIP.2.1)

- مکانیزم تشخیص صحت داده بر روی جداول زیر پیاده سازی شده است و نحوه اطلاع رسانی آنها شرح داده شده است:

TBL_User
Table Fields (UserName + MainParty + NationCode)

با دستکاری یکی از فیلدهای بالا از طریق جدول اطلاعات کاربران در پایگاه داده، در صورتیکه کاربری که اطلاعاتش دستکاری شده بخواهد در سامانه وارد شود، جلوی ورودش به سامانه گرفته شده و پیغامی که نشانگر دستکاری داده ها می باشد در صفحه لاگین نمایش داده می شود. همچنین لاگ مرتبطی برای ورود ناموفق این کاربر که نشان دهنده دستکاری اطلاعات هست در بخش گزارش رخدادنگاری جهت اطلاع رسانی به مدیر ثبت خواهد شد.

TBL_Setting
Table Fields (Key + Value)

با دستکاری یکی از فیلدهای بالا از طریق جدول مذکور در پایگاه داده، که در واقع موارد تنظیمات امنیتی سامانه می باشند رکورد ممیزی با عنوان "عدم اعتبار داده" در سامانه ثبت خواهد شد. رکورد ممیزی مذکور تا زمانیکه مدیر مجددا تنظیمات دستکاری شده را بروزرسانی نماید در فواصل زمانی جهت اطلاع رسانی به مدیر سامانه در لاگ ثبت می شود.

TBL_Treatment applicant

Table Fields (BirthDate + HasValidCardRegisterTime + Identifier)

در صورت تغییر غیرمجاز در هر یک از فیلدهای بالا، رکورد متقاضی درمان مربوطه در لیست متقاضیان فعال مرکز با رنگ قرمز مشخص خواهد شد.

فیلد HasValidCardRegisterTime می تواند دارای مقادیر ۱ یا ۲ یا ۳ باشد.

۱: دارای کد ملی احراز شده براساس اوراق هویت است.
۲: طبق احراز دارای کد ملی است.
۳: کد ملی ندارد.

در صورت دستکاری فیلد HasValidCardRegisterTime از جدول مربوط به متقاضیان مراکز، وقتی به بخش "برنامه درمان-- > تجویز دارو " متقاضی که اطلاعاتش دستکاری شده است مراجعه می کنیم. مقدار فیلد دوز دارو تغییر می کند.

رکورد لاگ با عنوان "پارامترهای اطلاعاتی مهم متقاضی درمان دستکاری شده است، شماره متقاضی ..... " در بخش گزارش رخدادنگاری ثبت خواهد شد. (FDP_SDI.2.2،FDP_SDI.2.1)

کلاس مدیریت امنیت

- محصول امکان فعال و غیرفعال نمودن کارکردهای تنظیمات امینتی سامانه توسط مدیرسامانه را دارد. این کارکردها شامل ثبت انواع داده ممیزی، ایجاد محدودیت های زمانی و محدودیت IP ،..... است. (FMT_MOF.1.1)
- محصول قابلیت تعیین مشخصه امنیتی را توسط مدیر سامانه دارد. در صورت عدم تنظیم مقادیر مشخصه‌های امنیتی مانند تلاش ناموفق برای ورود از مقادیر پیش‌فرض استفاده می‌نماید. این مقادیر قابل تغییر توسط مدیرسامانه هستند. (FMT_MSA.1.1، FMT_MSA.3.1، FMT_MSA.3.2)
- محصول قابلیت اختصاص و یا حذف نقش‌های موجود در سامانه به کاربران، پرس و جو گزارش رخدادنگاری و تغییر در داده های احراز هویت کاربران توسط مدیرسامانه را دارد. میزان دسترسی به اطلاعات در هر نقش از پیش تعریف شده است و مدیرسامانه جهت مدیریت دسترسی کاربران به اطلاعات میبایست نقش آنها را تغییر دهد. کاربران عادی در سامانه می توانند رمز عبور خود را تغییر بدهند و یا در صورت فراموشی رمز عبور خود را بازیابی نمایند. ((1) FMT_MTD.1.1، (2) FMT_MTD.1.1)
- محصول قادر است کارکردهای امنیتی زیر را اعمال نماید. (FMT_SMF.1.1)
  - کاربران با نقش ممیز برای خواندن اطلاعات رکوردهای ممیزی
  - پشتیبانی از مجوز مشاهده رویدادهای ممیزی
  - پشتیبانی از حد آستانه و از عملیات (حذف) در زمان خرابی ذخیره‌سازی ممیزی
  - پشتیبانی از عملیات (حذف) در زمان خرابی ذخیره‌سازی ممیزی
  - مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
  - مدیریت اجرای حفاظت از اطلاعات باقی‌مانده (آزاد سازی فضا) که در محصول قابل پیکربندی می‌باشد.
  - ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
  - مدیریت عملیات تشخیص صحت داده
  - مدیریت حدآستانه برای تلاش ناموفق احراز هویت
  - مدیریت پیچیدگی رمز عبور
  - امکان مدیریت نحوه و ایجاد محدودیت در احراز هویت
  - مدیرسامانه امکان تعیین دسترسی موجودیتهای فعال را دارد و محصول به صورت پیشفرض کاربران هیچگونه دسترسی ندارند.
  - امکان مدیریت کاربران و نقش آنها
  - امکان مدیریت شرایط آغاز نشست توسط مدیرسامانه

- امکان تعیین مدت زمان خاتمه نشست غیرفعال

- محصول دارای نقش‌های مدیرسامانه، کاربر دانشگاه علوم پزشکی ، کاربر معاونت غذا و دارو ، کاربر وزارت بهداشت ، کاربر سازمان غذا و دارو ، پشتیبان سیستم، روانشناس، پزشک-مسئول فنی، پرستار، درمانگر، مددکار، موسس مرکز درمانی، ارزیابی الکل، کاربر فرم کاهش آسیب، کاربرمبارزه با ستاد مبارزه با مواد مخدر و ممیز است. (FMT_SMR.1.1)
- محصول قادر به تعیین نقش کاربران توسط مدیرسامانه است. (FMT_SMR.1.2)

کلاس حفاظت از داده توابع امنیتی هدف امنیتی

- محصول در زمان بروز شکست‌های نرم افزاری پیغام مناسب داده و به فعالیت خود ادامه نمی‌دهد. (FPT_FLS.1.1)
- محصول از پروتکل‌های امن برای برقراری ارتباط با پایگاه داده استفاده می نماید. محصول در زمان اشتراک‌گذاری و یا تبادل اطلاعات از پروتکل های امن استفاده می نماید. (FPT_ITT.1.1، FPT_TDC.1.1، FPT_TDC.1.2)
- محصول قادر به تولید مهرهای زمانی برای تعیین زمان ایجاد داده‌های ممیزی می باشد. (FPT_STM.1.1)

کلاس تخصیص منابع

- در صورت بروز مشکلات سخت افزاری و یا سیستم عاملی محصول دچار شکست نرم افزاری خواهد گردید. (FRU_FLT.1.1)

کلاس دسترسی به هدف ارزیابی

- در این محصول امکان برقراری نشست همزمان وجود دارد و توسط مدیر تنظیم می‌شود. کلیه نشست های فعال محصول پس از مدت زمان تعیین شده توسط مدیر سامانه خاتمه خواهند یافت. کاربران سامانه با دکمه خروج که کاملا در دسترسی در تمامی صفحات سامانه امکان خاتمه دادن به نشست خود را دارند. (FTA_MCS.1.1، FTA_MCS.1.2، FTA_SSL.3.1، FTA_SSL.4.1)
- محصول قادر است پس از برقراری نشست موفقیت‌آمیز تلاش‌های ناموفق برقراری نشست را با نمایش روز و ساعت، و تعداد تلاش را به کاربران نمایش دهد. این اطلاعات جهت مشاهده کاربران در اختیار آنها قرار می گیرد. محصول امکان ایجاد محدودیت جهت برقرار نشست براساس IP، شناسه کاربری، نقش و محدوده زمانی را دارد. در ضمن تعداد تلاش‌های ناموفق جهت برقراری نشست قابل تنظیم است و پس از عبور از تعداد تعیین شده کاربر مورد نظر مسدود خواهد شد.(FTA_TAH.1.1 ، FTA_TAH.1.2، FTA_TAH.1.3، FTA_TSE.1.1)

کلاس کانال‌ها و مسیرهای امن

- محصول قادر است از پروتکل TLS جهت ایجاد زیرساخت امن ارتباطی بین خود و کاربران استفاده نماید. در ضمن قادر است کاربر را احراز هویت نموده و از تغییر و افشای اطلاعات درحال تبادل حفاظت نماید. این امکان برای مدیر سیستم نیز مهیا و الزامی است. (FTP_TRP.1.1، FTP_TRP.1.2، FTP_TRP.1.3)
- محصول از پروتکل امن ارتباطی TLS جهت ارتباط خود با سرور پیام کوتاه استفاده می نماید. محصول از ارسال پیام کوتاه برای ارسال هشدار حد آستانه و احرازهویت دو مرحله‌ای استفاده می‌کند. (FTP_ITC.1.1، FTP_ITC.1.2، FTP_ITC.1.3)

۷- توجیهات

الزامات زیر برای محصول کاربرد نداشته و در محدودیت ارزیابی قرار می‌گیرند:

کلاس حفاظت از داده‌های کاربری

- مولفه های FDP_ITC.2.1 و FDP_ITC.2.2 و FDP_ITC.2.3 و FDP_ITC.2.4 و FDP_ITC.2.5

در این سامانه برای ورود داده‌ها توسط کاربران از امضای دیجیتال بهره گرفته نمی‌شود و این مولفه برای سامانه کاربردی ندارد.

- مولفه FDP_ETC.2.1 و FDP_ETC.2.2 و FDP_ETC.2.3 و FDP_ETC.2.4

ورود داده‌های کاربری و در نتیجه خروج داده‌ی کاربری در این سامانه با مشخصه‌های امنیتی همراه نیست و این مولفه برای سامانه کاربردی ندارد.

کلاس حفاظت از توابع امنیتی هدف ارزیابی

- مولفه های FPT_TUD_EXT.1.2 و FPT_TUD_EXT.1.3

این الزام در محصول تحت وب کاربرد ندارد.