

به نام خدا

سند هدف امنیتی

سامانه مدیریت بیماریهای نادر - RDA

نسخه ۱,۰,۰

شرکت بهپرداز جهان

دی ماه ۱۴۰۰

نسخه ۱,۱

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- نرم افزار/سخت افزار/میان افزار 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- نیازمندی های امنیتی..... ۱۳
- ۵-۱- الزامات کارکرد امنیتی بر اساس پروفایل حفاظتی تحت شبکه..... ۱۴

- ۱-۱-۵- کلاس ممیزی امنیت ۱۸
- ۱-۲-۵- کلاس پشتیبانی از رمزنگاری ۲۱
- ۱-۳-۵- کلاس شناسایی و احراز هویت ۲۴
- ۱-۴-۵- کلاس حفاظت از داده کاربری ۲۸
- ۱-۱-۵- کلاس مدیریت امنیت ۳۲
- ۱-۲-۵- کلاس حفاظت از توابع امنیتی هدف ارزیابی ۳۶
- ۱-۳-۵- کلاس تخصیص منابع ۳۷
- ۱-۴-۵- کلاس دسترسی به هدف ارزیابی ۳۸
- ۱-۵-۵- کلاس کانالها و مسیرهای مورد اعتماد ۳۸
- ۲-۵- الزامات تضمین امنیتی براساس پروفایل حفاظتی تحت شبکه ۴۰
- ۶- خلاصه مشخصات هدف ارزیابی ۴۱
- ۷- توجیهات ۵۲

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه مدیریت بیماریهای نادر - RDA
نسخه	۱,۱
تاریخ	آبان ۱۴۰۰
نویسندگان	شرکت بهپرداز جهان

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت بهپرداز جهان
نام محصول	سامانه مدیریت بیماریهای نادر - RDA
نوع محصول	برنامه کاربردی تحت شبکه
نسخه	۱,۰,۰

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

- ۱- ثبت رویدادهای امنیتی
- ۲- ذخیره پسورها در پایگاه داده با بهره‌گیری از الگوریتم‌های استاندارد
- ۳- کنترل دسترسی بر روی داده‌ها و صفحات مدیریتی
- ۴- احراز هویت کاربران مبتنی بر شناسه‌ی کاربری و پسورد
- ۵- امکان انجام تنظیمات امنیتی، نظیر مدیریت کاربران، نقش‌ها و ...

۱-۳-۲- نوع هدف ارزیابی

برنامه کاربردی تحت وب

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

در جدول زیر سخت‌افزار، نرم‌افزار و میان‌افزارهای لازم برای کارکرد محصول بیان شده است:

حداقل الزامات	کامپوننت‌های محیط عملیاتی
Internet Explorer- Google Chrome	مرورگر

CentOS Linux release 7.9.2009 (Core) – Windows Server	سیستم عامل
IIS 10.0	وب سرور
Oracle Database 12c Enterprise Edition Release 12.2.0.1.210420	پایگاه داده
Microsoft .Net Framework 4.7.2	فریم ورک
Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz (VMware)	CPU
Oracle Database 12c Enterprise Edition Release 12.2.0.1.210420	RAM
۱۰۰ GB as /u01 & 500 GB as ASM +DATAGRP	HDD

۴-۱- توصیف هدف ارزیابی

هدف از سامانه ثبت نام بیماران گروه های هدف (پیوند، ام اس، تالاسمی، هموفیلی، CF، دیابت و ...) و نوع دارو و میزان داروی مصرفی آنها می باشد تا ضمن امکان سهمیه بندی دقیق داروهای خاص مورد نیاز و توزیع مناسب آن، مصرف منطقی دارو انجام گرفته و از سوء استفاده و قاچاق معکوس جلوگیری شود. ضمناً برخی خدمات مختص بیماران نادر نیز در این سامانه ثبت می گردد.

اجزای اصلی:

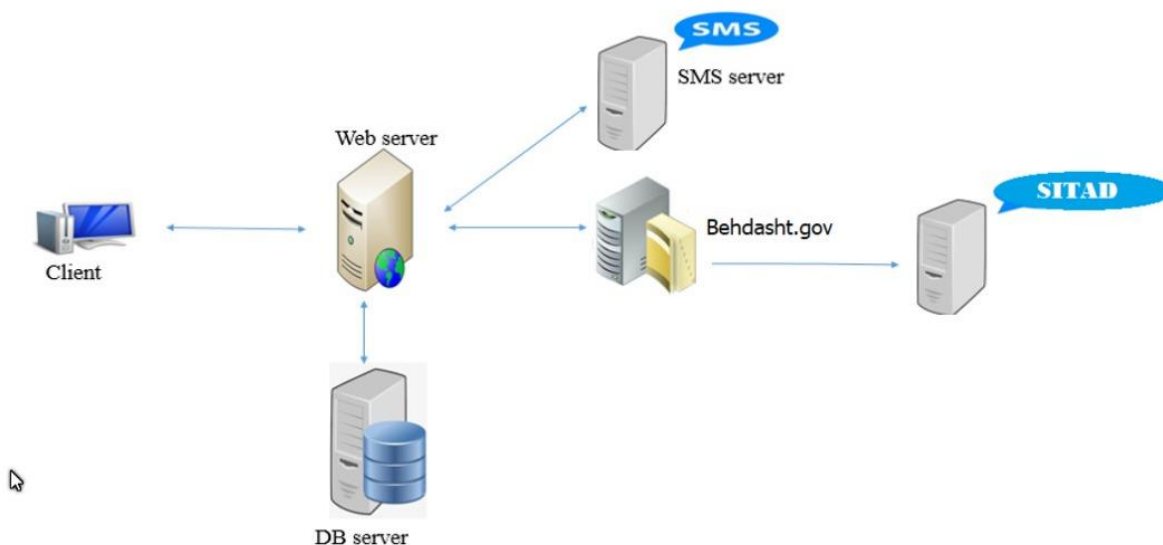
- اطلاعات پایه
- ثبت پرونده بیمار
- ثبت مجوز تحویل فرآورده
- ثبت درخواست انفصال پرونده
- ثبت تسهیلات
- گزارشات
- جستجوی پرونده دیابت

۴-۱-۱- حوزه فیزیکی

عناصر سخت افزاری و نرم افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می شود:

شماره مدل یا نسخه	عناصر محصول
10.0	IIS (Internet Information Services)
1.0.0	سامانه مدیریت بیماریهای نادر - RDA
12.2.0.1.210420	پایگاه داده Oracle Database 12c Enterprise

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 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 احراز هویت	به منظور شناسایی و احراز هویت 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.

کارکردها	توصیف
دسترسی به محصول	پالیسی های امنیتی در رابطه با نشست های برقرار شده با محصول لحاظ گردیده است.
کانال ها/ مسیرهای مورداعتماد	جهت جلوگیری از شنود و گم شدن داده ها در هنگام انتقال، از پروتکل https به همراه گواهینامه معتبر برای انتقال داده بین کاربر و سرور استفاده می شود.

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

توصیف	تهدید
<p>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.</p>	<p>T.UNAUTHORIZED_ACCESS</p>
<p>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 درصد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا کند.</p>	<p>T.DATA_ALTERATION</p>
<p>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 اضافه کردن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه کند.</p>	<p>T.REPUDIATION</p>
<p>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</p>	<p>T.DATA_DISCLOSURE</p>

توصیف	تهدید
عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.	
مهاجم میتواند سبب گردد محصول در یک بازه زمانی غیرقابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواستهای بسیار در یک بازه زمانی کوتاه صورت میگیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع 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.DENIAL_OF_SERVICE
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.HARMFUL_DATA
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.ELEVATION_OF_PRIVILEGES
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.	T.NETWORK_EAVESDROP

۳-۱-۲- فرضیات

توصیف	فرضیه
فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال می نمایند.	A.TRUSTED_ADMIN
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 می نمایند.	A.TRUSTED_DEVELOPER
فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب-پذیری های شناخته شده را اتخاذ می نمایند.	A.EXPERIENCED_DEVELOPER
فرض شده است که تمام پیش بینی های محیطی و فیزیکی لازم برای	A.SECURE_ENVIRONMENT

توصیف	فرضیه
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.	
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.PROPER_BACKUP
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 در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.	A.COMMUNICATION
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.SECURE_DELIVERY
فرض شده است که اقدامات امنیتی لازم در قبال حملات DDos اتخاذ می‌شود.	A.DIST_DENIAL_OF_SERVICE

۳-۱-۳- خط‌مشی

توصیف	خط‌مشی
تمام رخدادهای 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.COMPLEMENTARY_AUDIT
پیکربندی پیش‌فرض محصول و مولفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش‌فرض، خطاهای پیش‌فرض و صفحات 404، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خط‌مشی سازمانی بسیار مهم است به خصوص زمانی که	P.PROPER_CONFIGURATION

توصیف	خطمشی
محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.	
امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تأیید موجود باشد.	P.E_SIGNATURE

۴- اهداف امنیتی

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

۴-۱-۱- اهداف امنیتی برای هدف ارزیابی

توصیف	هدف امنیتی
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.AUDIT
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 طوری که کاربران را ملزم به استفاده از کلمه‌های 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 احراز هویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت براساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.	O.AUTH
محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف شده می‌تواند بیانگر حمله DoS	O.DATA_FLOW_CONTROL

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 کارآمد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط‌های مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش‌های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش‌ها و مجوزهایی تنظیم نماید.
O.ERROR_MANAGEMENT	محصول باید صورت امن و کارآمد 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.

۴-۱-۲- 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

توصیف	هدف امنیتی
غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده شده اشاره نمود.	
محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.	OE.COMMUNICATION
محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.	OE.TRUSTED_ADMIN
محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.	OE.TRUSTED_DEVELOPER
محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.	OE. EXPERIENCED_DEVELOPER
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.COMPLEMENTARY_AUDIT
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. SECURE_DELIVERY
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.	OE. PROPER_BACKUP

۵- نیازمندی‌های امنیتی

۱-۵- 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		
۱۶		FCS_TLSC_EXT.1: الزامات پروتکل TLS Client ۱
۱۷		
۱۸		FCS_TLSC_EXT.4: الزامات پروتکل TLS Client ۴
۱۹		
۲۰		FCS_TLSS_EXT.1: الزامات پروتکل TLS Server
۲۱		
۲۲	FDP: حفاظت از داده کاربری	FDP_ACC.1: خط مشی کنترل دسترسی
۲۳		
۲۴		FDP_ACF.1: عملیات کنترل دسترسی
۲۵		

		۲۶
FDP_RIP.2 : حفاظت کامل از اطلاعات باقیمانده در منابع		۲۷
FDP_ITC.2 : ورود داده کاربری به محصول با مشخصه امنیتی		۲۸
		۲۹
		۳۰
		۳۱
		۳۲
FDP_ETC.2 : خروج داده کاربری از محصول با مشخصه امنیتی		۳۳
		۳۴
		۳۵
		۳۶
FDP_SDI.1 : صحت داده کاربری ذخیره شده		۳۷
		۳۸
FIA : شناسایی و احراز هویت	FIA_AFL.1 : مدیریت احراز هویت ناموفق	۳۹
	FIA_ATD.1 : تعریف مشخصات کاربر	۴۰
	FIA_PMG_EXT.1 : مدیریت کلمه عبور	۴۱
	FIA_UAU.2 : احراز هویت قبل از هر اقدام	۴۲
	FIA_UID.2 : شناسایی قبل از هر اقدام	۴۳
	FIA_UAU.5 : سازوکار احراز هویت چندگانه	۴۴
		۴۵
		۴۶
	FIA_USB.1 : انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	۴۷
		۴۸
		۴۹
	FIA_X509_EXT.1 : اعتبارسنجی گواهی x509	۵۰
		۵۱
FIA_X509_EXT.2 : احراز هویت از طریق گواهی X509	۵۲	
	۵۳	
FMT : مدیریت امنیت	FMT_MOF.1 : مدیریت کارکرد در محصول	۵۴
	FMT_MSA.1 : مدیریت مشخصه های امنیتی	۵۵
	FMT_MSA.3 : مقداردهی ایستای مشخصه های امنیتی	۵۶
		۵۷

FMT_MTD.1(1): مدیریت داده‌های توابع امنیتی هدف ارزیابی (مدیر سیستم)	۵۸
FMT_MTD.1(2): مدیریت داده‌های توابع امنیتی هدف ارزیابی (کاربر عادی، وارد کننده داده)	۵۹
FMT_SMF.1: کارکردهای مدیریتی محصول	۶۰
FMT_SMR.1: نقشهای امنیتی	۶۱
FPT_FLS.1: حفظ وضعیت امن در زمان شکست	۶۳
FPT_ITT.1: انتقال داده امنیتی در داخل محصول	۶۴
FPT_TDC.1.2: سازگاری داده امنیتی بین محصول و موجودیت امن	۶۵
FPT_STM.1: مهرهای زمانی	۶۶
FPT_TUD_EXT.1: به روزرسانی امن	۶۷
FPT_TUD_EXT.1: به روزرسانی امن	۶۸
FPT_TUD_EXT.1: به روزرسانی امن	۶۹
FRU_FLT.1: تحمل خطا	۷۰
FTA_MCS.1: محدودیت بر روی چندین نشست همزمان	۷۱
FTA_MCS.1: محدودیت بر روی چندین نشست همزمان	۷۲
FTA_SSL.3: خاتمه دادن به نشستها توسط محصول	۷۳
FTA_SSL.4: خاتمه دادن به نشستها توسط کاربر	۷۴
FTA_TAH.1: سوابق دسترسی به محصول	۷۵
FTA_TAH.1: سوابق دسترسی به محصول	۷۶
FTA_TAH.1: سوابق دسترسی به محصول	۷۷
FTA_TSE.1: برقراری نشست	۷۸
FTP_TRP.1: مسیر امن	۷۹
FTP_TRP.1: مسیر امن	۸۰
FTP_TRP.1: مسیر امن	۸۱
FTP_ITC.1: کانال امن	۸۲
FTP_ITC.1: کانال امن	۸۳
FTP_ITC.1: کانال امن	۸۴
عملیات رمزنگاری - رمزنگاری و رمزگشایی ۱ (۳)	۸۵
الزامات پروتکل TLS Server / احراز هویت (۴)	۸۶



الزامات پروتکل TLS Server / احراز هویت (۵)		۸۷
الزامات پروتکل TLS Server / احراز هویت (۶)		۸۸

۱-۱-۵- کلاس ممیزی امنیت

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید: <ul style="list-style-type: none"> • 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. 	FAU_GEN.1.1	۱	FPT_STM.1	FAU_GEN.1
محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: <ul style="list-style-type: none"> • 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.1.2	۲		
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_GEN.2.1	۳	FAU_GEN.1 FIA_UID.1	FAU_GEN.2
بازبینی داده ممیزی ۱: محصول باید امکان خواندن [کلیه داده‌های ممیزی] از کل رکوردهای ممیزی را برای [مدیر سیستم] فراهم نماید.	FAU_SAR.1.1	۴	FAU_GEN.1	FAU_SAR.1
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.1.2	۵		
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.2.1	۶	FAU_SAR.1	FAU_SAR.2
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، IP، سطوح رویداد، نوع رویداد] مرتب نماید.	FAU_SAR.3.1	۷	FAU_SAR.1	FAU_SAR.3
محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادهای جهت ممیزی شدن، انتخاب نماید:	FAU_SEL.1.1	۸	FAU_GEN.1 FMT_MTD.1	FAU_SEL.1

				<ul style="list-style-type: none"> • [نوع رخداد] • [هیچ معیار دیگری]
محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی راه، از حذف غیرمجاز حفاظت نماید.	FAU_STG.1.1	۹	FAU_GEN.1	FAU_STG.1
محصول باید قادر به [تشخیص] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آنها باشد.	FAU_STG.1.2	۱۰		
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.3.1	۱۱	FAU_STG.1	FAU_STG.3
محصول در صورت پر شدن دنباله ممیزی، باید [روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید] و [هیچ اقدام دیگری].	FAU_STG.4.1	۱۲	FAU_STG.1	FAU_STG.4

جدول ۱- لیست رویدادهای قابل ممیزی

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

	(پایه)	
	ثابت کاربرد ناموفق از سازوکار احراز هویت (حداقل) ثابت تمام کاربردهای سازوکار احراز هویت (پایه)	FIA_UAU.1
	ثابت نتایج احراز هویت (حداقل) ثابت هر سازوکار احراز هویت فعال همراه با نتیجه نهائی (پایه)	FIA_UAU.5
شناسه کاربر شامل آدرس مبدا، شناسایی نقطه پایانی اتصال	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	FIA_UID.1
برای مثال، رد و یا قبول کلمه عبور کاربر	ثابت رد هر کلمه عبور تست شده توسط محصول (حداقل) ثابت تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول (پایه)	FIA_PMG_EXT.1
	ثابت 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)	FIA_USB.1
	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	FMT_MSA.1
به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	FMT_MTD.1(1)
به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	FMT_MTD.1(2)
	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(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)
شناسایی داده‌های موجودیت غیرفعال	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول	FDP_ACF.1

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

۲-۱-۵- کلاس پشتیبانی از رمزنگاری

شرح المان	المان	شماره	وابستگی ها	مؤلفه
محصول باید [برای واریسی صحت داده‌های ممیزی و داده‌های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [SHA256] و اندازه کلید رمزنگاری [۲۵۶] اجرا شود که مطابق با [FIPS 180-3] باشد.	FCS_COP.1.1(1)	۱	FDP_ITC.1 FDP_ITC.2 FCS_CKM.1	FCS_COP.1(1)
محصول باید [تولید داده درهم‌سازی] بر اساس یک الگوریتم رمزنگاری مشخص [SHA256] و اندازه-کلید رمزنگاری [۲۵۶] اجرا شود که مطابق با [FIPS 180-3] باشد.	FCS_COP.1.1(2)	۲	FDP_ITC.1 FDP_ITC.2 FCS_CKM.1	FCS_COP.1(2)
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: _	FCS_TLSC_EXT.1.1	۳	-	FCS_TLSC_EXT.1

شرح المان	المان	شماره	وابستگی ها	مؤلفه
]				
محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.	FCS_TLSC_EXT.1.2	۴		
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی نامه سرور برقرار سازد. اگر گواهی نامه سرور غیرمعتبر به نظر رسید، محصول باید [ارتباط را برقرار نسازد]	FCS_TLSC_EXT.1.3	۵		
محصول باید در پیام <u>Client Hello</u> [Supported Elliptic Curves Extension] را به همراه <u>NIST curve</u> های [secp256r1, secp384r1 secp521r1] و هیچ منحنی دیگری ارائه کند.]	FCS_TLSC_EXT.4.1	۶	-	FCS_TLSC_EXT.4

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
<p><u>خود استفاده کنند.</u></p> <ul style="list-style-type: none"> • <u>بارگذاری جواب آزمایش ژنتیک</u> • <u>دانلود و مشاهده فایل و ویدئوهای آموزشی</u> • <u>هیچ اقدام دیگری</u>] 				
<p>محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احراز هویت نماید.</p>	FIA_UAU.1.2	۶	-	FIA_UAU.1
<p>سازوکار احراز هویت چندگانه ۱: محصول باید به منظور احراز هویت کاربر سازوکارهای زیر را فراهم آورد:</p> <ul style="list-style-type: none"> • نام کاربری و کلمه عبور • ارسال OTP از طریق ارسال پیام کوتاه به تلفن همراه 	FIA_UAU.5.1	۷		FIA_UAU.5
<p>محصول باید هر کاربر متقاضی احراز هویت را مطابق قوانین ذیل احراز هویت نماید:</p> <ul style="list-style-type: none"> • کاربران از راه دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه (مانند Dual factor authentication) استفاده کند. • [هیچ قانون دیگری] 	FIA_UAU.5.2	۸	-	
<p>محصول پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم می‌آورد:</p> <ul style="list-style-type: none"> • ارائه لیست مراکز درمانی دیابت • لیست بیماریهای نادر در اولویت واکسیناسیون • ارائه لینکی به بیماران دیابتی که می‌توانند از آن برای اطمینان از ثبت کد ملی و صحت اطلاعات 	FIA_UID.1.1	۹	-	FIA_UID.1

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
<p>خود استفاده کنند.</p> <ul style="list-style-type: none"> • بارگذاری جواب آزمایش ژنتیک • دانلود و مشاهده فایل و ویدئوهای آموزشی [
<p>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.</p>	FIA_UID.1.2	۱۰	-	FIA_UID.1
<p>محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:</p> <ul style="list-style-type: none"> • شناسه کاربر • نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه • جزئیات واسط کلاینت • پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق) • [هیچ مشخصه دیگری] 	FIA_USB.1.1	۱۱		
<p>محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:</p> <ul style="list-style-type: none"> • زمانی که 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] 	FIA_USB.1.2	۱۲	FIA_ATD.1	FIA_USB.1
<p>محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید:</p> <ul style="list-style-type: none"> • هیچ تغییری در طول نشست فعال مجاز نمی‌باشد، 	FIA_USB.1.3	۱۳		

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
<ul style="list-style-type: none"> • [هیچ قانون دیگری] 				
<p>محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند:</p> <ul style="list-style-type: none"> • 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» تنظیم شده است • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از <u>لیست فسخ گواهی‌نامه (CRL)</u> مشخص شده در <u>RFC 5759 بخش ۵</u> تأیید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند: <ul style="list-style-type: none"> ○ گواهی‌نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (3 id-kp 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" (1 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" (2 id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند. 	FIA_X509_EXT.1.1	۱۴	-	FIA_X509_EXT.1

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
○ 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.				
محصول مورد ارزیابی تنها در صورتی که 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.1.2	۱۵		
محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای [TLS]، و [ارسال OTP احراز هویت] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.	FIA_X509_EXT.2.1	۱۶		FIA_X509_EXT.2
در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید [گواهی را نپذیرد].	FIA_X509_EXT.2.2	۱۷	-	FIA_X509_EXT.2

۴-۱-۵- کلاس حفاظت از داده کاربری

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
محصول باید [خط‌مشی‌های کنترل دسترسی] را بر روی موارد زیر اعمال نماید: • موجودیت فعال: [مدیر سیستم، کاربر عادی، کارشناس ناظر بهداشت، کارشناس دیابت]]	FDP_ACC.1.1	۱	FDP_ACF.1	FDP_ACC.1

شرح المان	المان	شماره	وابستگی ها	مؤلفه
<ul style="list-style-type: none"> • موجودیت غیرفعال: رکوردها، مستندات و فرا-داده^۱ داده متعلق به کاربران داده احراز هویت 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] 				
<p>محصول باید [خطمشی‌های کنترل دسترسی] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید:</p> <ul style="list-style-type: none"> • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند • [هیچ مشخصه دیگری] 	FDP_ACF.1.1	۲	FDP_ACC.1 FMT_MSA.3	FDP_ACF.1

^۱ Metadata

شرح المان	المان	شماره	وابستگی ها	مؤلفه
<p>محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید:</p> <p>]</p> <p>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.</p> <p>[</p>	FDP_ACF.1.2	۳		
<p>محصول باید براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد:</p> <p>]</p> <ul style="list-style-type: none"> • 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] <p>[</p>	FDP_ACF.1.3	۴		
<p>محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید:</p> <p>]</p> <p>تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده،</p> <p>[هیچ قانون دیگری]</p>	FDP_ACF.1.4	۵		
<p>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.</p>	FDP_RIP.2.1	۶	-	

شرح المان	المان	شماره	وابستگی ها	مؤلفه
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.	FDP_SDI.2.1	۷	- -	FDP_SDI.2
هنگام تشخیص خطای صحت داده، محصول باید [نمایش پیام در برنامه و ثبت رکورد لاگ جهت اطلاع رسانی به مدیر] را صورت دهد.	FDP_SDI.2.2	۸		

^۲ Hash

۱-۱-۵- کلاس مدیریت امنیت

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه
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_MOF.1.1	۱	FMT_SMR.1 FMT_SMF.1	FMT_MOF.1
محصول باید با اعمال [خطمشی کنترل دسترسی]، [امکان تغییر پیش فرض، پرس و جو، تغییر، حذف، [هیچ عملیات دیگری]] مشخصه‌های امنیتی] <ul style="list-style-type: none"> • شناسه کاربر • نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه • جزئیات واسط کلاینت • پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق) • [هیچ مشخصه دیگری] [را به [مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود نماید.	FMT_MSA.1.1	۲	[FDP_ACC.1 , or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FMT_MSA.1
محصول برای مشخصه های امنیتی که برای اعمال [خط مشی کنترل دسترسی] استفاده می شوند، باید مقادیر پیش فرض محدود شده ای در نظر بگیرد.	FMT_MSA.3.1	۳	FMT_MSA.1 FMT_SMR.1	FMT_MSA.3
محصول برای تعیین مقادیر اولیه پیشنهادی باید به [مدیر سیستم] اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش فرض را لغو و تغییر دهد.	FMT_MSA.3.2	۴		
محصول باید توانایی [تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، [هیچ کارکرد دیگری]] رویدادهای متمایز سیستم، مجوزهای نقش و دسترسی، داده‌های احراز هویت و تنظیمات امنیتی] را به [مدیر سیستم] محدود نماید.	FMT_MTD.1.1 (1)	۵	FMT_SMR.1 FMT_SMF.1	FMT_MTD.1
محصول باید توانایی [تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، [هیچ کارکرد دیگری]] [تغییر رمز عبور] را به [کاربر عادی] محدود نماید.	FMT_MTD.1.1 (2)	۶		

شرح المان	المان	شماره	وابستگی‌ها	مؤلفه																				
محصول باید قادر به انجام [کارکردهای مدیریتی که در جدول زیر آمده است] باشد:																								
<table border="1"> <thead> <tr> <th>عملیات مدیریتی</th> <th>مؤلفه</th> </tr> </thead> <tbody> <tr> <td>پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی</td> <td>FAU_GEN.1</td> </tr> <tr> <td>پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی</td> <td>FAU_SEL.1</td> </tr> <tr> <td>پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی</td> <td>FAU_STG.3</td> </tr> <tr> <td>پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی</td> <td>FAU_STG.4</td> </tr> <tr> <td>مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع</td> <td>FDP_ACF.1</td> </tr> <tr> <td>انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پی‌کربندی باشد.</td> <td>FDP_RIP.2</td> </tr> <tr> <td>ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول</td> <td>FDP_ITC.2</td> </tr> <tr> <td>عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پی‌کربندی باشد.</td> <td>FDP_SDI.1</td> </tr> <tr> <td>مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.</td> <td>FIA_AFL.1</td> </tr> </tbody> </table>	عملیات مدیریتی	مؤلفه	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی	FAU_GEN.1	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	FAU_SEL.1	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	FAU_STG.3	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	FAU_STG.4	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع	FDP_ACF.1	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پی‌کربندی باشد.	FDP_RIP.2	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	FDP_ITC.2	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پی‌کربندی باشد.	FDP_SDI.1	مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.	FIA_AFL.1	FMT_SMF.1.1	۷	-	FMT_SMF.1
عملیات مدیریتی	مؤلفه																							
پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی	FAU_GEN.1																							
پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	FAU_SEL.1																							
پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	FAU_STG.3																							
پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	FAU_STG.4																							
مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع	FDP_ACF.1																							
انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پی‌کربندی باشد.	FDP_RIP.2																							
ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	FDP_ITC.2																							
عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پی‌کربندی باشد.	FDP_SDI.1																							
مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.	FIA_AFL.1																							

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

شرح المان		المان	شماره	وابستگی‌ها	مؤلفه
مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.	FMT_SMR.1				
مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر	FTA_MCS.1				
مدیریت شرایط آغاز نشست توسط مدیر مجاز	FTA_TSE.1				
تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.	FTA_SSL.3				
نقش‌های زیر در محصول باید تعریف شده باشد: [مدیر سیستم، کاربر عادی، [هیچ نقش دیگری]]		FMT_SMR.1.1	۸	FIA_UID.1	FMT_SMR.1
محصول، باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند.		FMT_SMR.1.2	۹		

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

شرح المان	المان	شماره	وابستگی ها	مؤلفه
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [شکست‌های نرم‌افزاری، شکست‌های سخت‌افزاری]	FPT_FLS.1.1	۱	-	FPT_FLS.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_ITT.1.1	۲	FTP_TRP.1.1	FPT_ITT.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 ارسال پروتکل ارتباطی [FPT_TDC.1.1	۳	FTP_TRP.1.1	FPT_TDC.1
محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [از پروتکل TLS] استفاده نماید.	FPT_TDC.1.2	۴		
محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند.	FPT_STM.1.1	۵	-	FPT_STM.1

۳-۱-۵- کلاس تخصیص منابع

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

۴-۱-۵- کلاس دسترسی به هدف ارزیابی

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

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

^۳Remote

شرح المان	المان	شماره	وابستگی ها	مؤلفه
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 راه دور 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.1.1	۱	-	FTP_TRP.1
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	FTP_TRP.1.2	۲		
باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی نماید.	FTP_TRP.1.3	۳		
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 احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	FTP_ITC.1.1	۴	-	FTP_ITC.1
محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	FTP_ITC.1.2	۵		
محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای ارسال پیامک جهت احراز هویت ثانویه و هشدار به ادمین برای حدآستانه لاگ] راه اندازی نماید.	FTP_ITC.1.3	۶		

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 می-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 آماده سازی
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 مؤلفه های توسعه یافته
	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 آسیب پذیری

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 ثبت نماید و برای هر رکورد ممیزی، حداقل اطلاعات IP، تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال 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. در ضمن 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 و یا فیلتر نماید. (FAU_SAR.1.1، FAU_SAR.1.2، FAU_SAR.2.1، FAU_SAR.3.1)
- رویدادهای ممیزی دارای سطح بندی حساس، مهم و عادی هستند، در ادامه لیستی از این سطح بندی ارائه شده است. مدیر سیستم می‌تواند رویدادنگاری از این سطوح را فعال یا غیرفعال نماید. (FAU_SEL.1.1)

LogType	LogAction	PersianTitle
Important	AuditLogAction.HealthCenterPartyUpdate	ویرایش متعامل مرکز درمانی
Important	AuditLogAction.DrugFrequencyUsageInformationUpdate	ویرایش تواتر مصرف دارو
Important	AuditLogAction.GenericResourceInsert	ثبت فرآورده ژنریک
Important	AuditLogAction.GenericResourceUpdate	ویرایش فرآورده ژنریک
Important	AuditLogAction.ResourceTypeInsert	ثبت نوع فرآورده
Important	AuditLogAction.ResourceTypeUpdate	ویرایش نوع فرآورده
Important	AuditLogAction.SicknessCenterPharmacyInsert	ثبت داروخانه مراکز سلامت
Important	AuditLogAction.SicknessCenterPharmacyUpdate	ویرایش داروخانه مراکز سلامت
Important	AuditLogAction.RDAUserInfoInsert	ثبت کاربر متعاملین
Important	AuditLogAction.RDAUserInfoUpdate	ویرایش کاربر متعاملین
Important	AuditLogAction.PasswordStrengthFailure	عدم پذیرش پسوندها (مکانیزم پیچیدگی پسوندها)
Important	AuditLogAction.AuditLogView	مشاهده رویدادهای سیستم تلاش ناموفق برای ورود به سامانه (مسدود موقت)
Important	AuditLogAction.UserLockedLoginFailed	تلاش ناموفق برای ورود به سامانه
Important	AuditLogAction.UserLoginFailed	خروج کاربر از حالت مسدود
Important	AuditLogAction.UserUnlocked	عدم رعایت تعداد همزمان ورود به سامانه
Important	AuditLogAction.ConcurrentSessionCountFailure	سامانه
Important	AuditLogAction.InvalidIPRange	با IP غیرمجاز تلاش برای ورود به سامانه در ساعت غیرمجاز
Important	AuditLogAction.LoginInInvalidLoginTime	خروج کاربر به علت حذف کاربر
Important	AuditLogAction.UserLogOffUserDelete	

Important	AuditLogAction.EbSicknessCaseView	مشاهده پرونده EB
Important	AuditLogAction.EbSicknessCaseChangeStatus	وضعیت پرونده و مجوز های EB مشاهده پرونده سایر بیماری های متابولیک
Important	AuditLogAction.MetabolicOtherSicknessCaseView	مشاهده پرونده MPS
Important	AuditLogAction.MPSSicknessCaseView	تغییر وضعیت پرونده و مجوز های MPS
Important	AuditLogAction.MPSSicknessCaseChangeStatus	دریافت گزارش مجوزهای تکراری
Important	AuditLogAction.SicknessCaseDuplicateLicenseReport	تحویل فرآورده
Important	AuditLogAction.SicknessCaseLicenseReport	دریافت گزارش مجوزهای بیماران خاص
Important	AuditLogAction.CFUniversityNebulizers	دریافت گزارش نبولایزر بیماران CF تلاش ناموفق برای ورود به سامانه - کد رد OTP
Important	AuditLogAction.OTPCodeNotAccepted	خروج کاربر به علت ویرایش دسترسی های نقش
Important	AuditLogAction.UserLogOffRoleChanged	خروج کاربر به علت حذف نقش
Important	AuditLogAction.UserLogoffDeleteRule	خروج کاربر به علت غیرفعال شدن نقش
Important	AuditLogAction.UserLogoffDeActiveRule	خروج کاربر به علت حذف انتساب دسترسی
Important	AuditLogAction.UserLogoffOperationDeleteAssign	خروج کاربر به دلیل حذف انتساب نقش
Important	AuditLogAction.UserLogoffRoleDeleteAssign	حمله XSS
Sensitive	AuditLogAction.XSSAttack	برای ورود به سامانه(مشکل شماره موبایل)
Sensitive	AuditLogAction.UserLoginFailedcauseMobile	تلاش برای ارسال پیامک تجاوز از حد آستانه رویداد ها
Sensitive	AuditLogAction.TryNotifyOnMaxOfAuditBySMS	حذف نظر پزشک معتمد - پرونده
Sensitive	AuditLogAction.TrustedDoctorOpinionStatusDelete	حذف پرونده پیوندی
Sensitive	AuditLogAction.TransplantSicknessCaseDelete	حذف پرونده تالاسمی
Sensitive	AuditLogAction.ThalassemiaSicknessCaseDelete	ویرایش سازمان بیمه گر
Sensitive	AuditLogAction.SupporterInsurerUpdate	حذف سازمان بیمه گر
Sensitive	AuditLogAction.SupporterInsurerDelete	خطا در ورود کاربر به سامانه
Sensitive	AuditLogAction.SomethingWrongWithUserLogin	حذف داروخانه مراکز سلامت
Sensitive	AuditLogAction.SicknessCenterPharmacyDelete	ویرایش پرونده بیماری
Sensitive	AuditLogAction.SicknessCaseTypeUpdate	ثبت پرونده بیماری
Sensitive	AuditLogAction.SicknessCaseTypeInsert	حذف پرونده بیماری
Sensitive	AuditLogAction.SicknessCaseTypeDelete	حذف تخفیف
Sensitive	AuditLogAction.SicknessCaseDiscountDelete	ویرایش تنظیمات امنیتی
Sensitive	AuditLogAction.SecuritySettingUpdate	ویرایش IP مجاز
Sensitive	AuditLogAction.SecurityIPRangeUpdate	ثبت IP مجاز
Sensitive	AuditLogAction.SecurityIPRangeInsert	حذف IP مجاز
Sensitive	AuditLogAction.SecurityIPRangeDelete	ویرایش نقش
Sensitive	AuditLogAction.RoleUpdate	تغییر در دسترسی های نقش
Sensitive	AuditLogAction.RoleOperationChange	ثبت نقش به صورت دسته ای
Sensitive	AuditLogAction.RoleOperationAddBatch	ثبت نقش
Sensitive	AuditLogAction.RoleInsert	حذف انتساب نقش
Sensitive	AuditLogAction.RoleDeleteAssign	حذف نقش
Sensitive	AuditLogAction.RoleDelete	

Sensitive	AuditLogAction.RoleAssign	انتساب نقش
Sensitive	AuditLogAction.ResourceTypeDelete	حذف نوع فرآورده
Sensitive	AuditLogAction.ResourceNatureTypeDelete	حذف ماهیت فرآورده
Sensitive	AuditLogAction.ResourceLevelDelete	حذف سطح گروه فرآورده
Sensitive	AuditLogAction.ResourceFormDelete	حذف شکل فرآورده
Sensitive	AuditLogAction.RDAUserInfoDelete	حذف کاربر متعاملین
Sensitive	AuditLogAction.PIDSicknessCaseDelete	حذف پرونده PID
Sensitive	AuditLogAction.PatientVerification	ارزیابی اطلاعات بیماران
Sensitive	AuditLogAction.PatientDelete	حذف اطلاعات بیمار
Sensitive	AuditLogAction.PasswordHashing	رمزنگاری گذرواژه
Sensitive	AuditLogAction.PartyIdentityUpdate	ویرایش اطلاعات متعاملین
Sensitive	AuditLogAction.PartyIdentityInsert	ثبت اطلاعات متعاملین
Sensitive	AuditLogAction.PartyIdentityDelete	حذف اطلاعات متعاملین
Sensitive	AuditLogAction.OtismSicknessCaseDelete	حذف پرونده اوتیسم
Sensitive	AuditLogAction.OperationUpdate	ویرایش دسترسی
Sensitive	AuditLogAction.OperationInsert	ثبت دسترسی
Sensitive	AuditLogAction.OperationDeleteAssign	حذف انتساب دسترسی
Sensitive	AuditLogAction.OperationDelete	حذف دسترسی
Sensitive	AuditLogAction.OperationAssign	انتساب دسترسی
Sensitive	AuditLogAction.OperationAddBatch	ثبت دسترسی به صورت دسته ای
Sensitive	AuditLogAction.OnMaxOfAudit	تجاوز از حد آستانه رویداد ها
		ارسال پیامک تجاوز از حد آستانه رویداد ها
Sensitive	AuditLogAction.NotifyOnMaxOfAuditBySMS	رویداد ها
Sensitive	AuditLogAction.MSSicknessCaseDelete	حذف پرونده ام اس
Sensitive	AuditLogAction.MPSSicknessCaseDelete	حذف پرونده MPS
		حذف پرونده سایر بیماری های متابولیک
Sensitive	AuditLogAction.MetabolicOtherSicknessCaseDelete	حذف نظر پزشک معتمد - مجوز
Sensitive	AuditLogAction.LicenseTrustedDoctorOpinionStatusDelete	حذف مجوز پرونده
Sensitive	AuditLogAction.JsonSicknessCaseLicenseDelete	حذف فرآورده ژنریک
Sensitive	AuditLogAction.GenericResourceDelete	حذف گروه ژنریک
Sensitive	AuditLogAction.GenericResourceCategoryDelete	حذف پرونده EB
Sensitive	AuditLogAction.EbSicknessCaseDelete	حذف نحوه مصرف دارو
Sensitive	AuditLogAction.DrugUsageInformationDelete	ویرایش مدیریت اسناد
Sensitive	AuditLogAction.DocumentTypeUpdate	ثبت مدیریت اسناد
Sensitive	AuditLogAction.DocumentTypeInsert	حذف مدیریت اسناد
Sensitive	AuditLogAction.DocumentTypeDelete	حذف اطلاعات پزشک
Sensitive	AuditLogAction.DoctorInfoDelete	حذف پرونده دیابت
Sensitive	AuditLogAction.DiabetSicknessCaseDelete	احتمال حمله XSS
Sensitive	AuditLogAction.ContingencyXSSAttack	تغییر رمز عبور
Sensitive	AuditLogAction.ChangePassword	حذف فرآورده تجاری
Sensitive	AuditLogAction.BrandResourceDelete	تلاش ناموفق برای دسترسی به
Sensitive	AuditLogAction.AuditLogAccessDenied	رویدادهای سیستم
	AuditLogAction.AgentInvalidLogOuted	خروج کاربر به دلیل عدم تطبیق
Sensitive		اطلاعات کاربر وارد شده

Sensitive	AuditLogAction.AuditLogCheckSumErr	تغییر غیرمجاز رویداد سیستم
Sensitive	AuditLogAction.UserInfoCheckSumErr	تغییر غیرمجاز اطلاعات کاربر
Sensitive	AuditLogAction.SicknessCaseCheckSumErr	تغییر غیرمجاز اطلاعات پرونده
Ordinary	AuditLogAction.UserSessionTimeout	اتمام نشست کاربر
Ordinary	AuditLogAction.UserLogOff	خروج کاربر از سامانه
Ordinary	AuditLogAction.TrustedDoctorOpinionStatusUpdate	ویرایش نظر پزشک معتمد - پرونده
Ordinary	AuditLogAction.TrustedDoctorOpinionStatusInsert	ثبت نظر پزشک معتمد - پرونده
Ordinary	AuditLogAction.TransplantSicknessCaseUpdate	ویرایش پرونده پیوندی
Ordinary	AuditLogAction.TransplantSicknessCaseInsert	ثبت پرونده پیوندی
Ordinary	AuditLogAction.ThalassemiaSicknessCaseUpdate	ویرایش پرونده تالاسمی
Ordinary	AuditLogAction.ThalassemiaSicknessCaseInsert	ثبت پرونده تالاسمی
Ordinary	AuditLogAction.SpecialityTypeUpdate	ویرایش انواع تخصص پزشک
Ordinary	AuditLogAction.SpecialityTypeInsert	ثبت انواع تخصص پزشک
Ordinary	AuditLogAction.SpecialityTypeDelete	حذف انواع تخصص پزشک
Ordinary	AuditLogAction.SpecialDrugBrandResourceUpdate	ویرایش برند فرآورده ژنریک
Ordinary	AuditLogAction.SpecialDrugBrandResourceInsert	ثبت برند فرآورده ژنریک
Ordinary	AuditLogAction.SimilarGenericResourceUpdate	ویرایش داروهای مشابه
Ordinary	AuditLogAction.SimilarGenericResourceInsert	ثبت داروهای مشابه
Ordinary	AuditLogAction.SimilarGenericResourceDelete	حذف داروهای مشابه
Ordinary	AuditLogAction.SicknessCaseDiscountInsert	ثبت تخفیف
Ordinary	AuditLogAction.SicknessCaseDisconnectionReject	رد درخواست انفصال
Ordinary	AuditLogAction.SicknessCaseDisconnectionInsert	ثبت درخواست انفصال
Ordinary	AuditLogAction.SicknessCaseDisconnectionCancel	ابطال درخواست انفصال
Ordinary	AuditLogAction.SicknessCaseDisconnectionAccept	تایید درخواست انفصال
Ordinary	AuditLogAction.ResourceNatureTypeUpdate	ویرایش ماهیت فرآورده
Ordinary	AuditLogAction.ResourceNatureTypeInsert	ثبت ماهیت فرآورده
Ordinary	AuditLogAction.ResourceLevelUpdate	ویرایش سطح گروه فرآورده
Ordinary	AuditLogAction.ResourceLevelInsert	ثبت سطح گروه فرآورده
Ordinary	AuditLogAction.ResourceFormUpdate	ویرایش شکل فرآورده
Ordinary	AuditLogAction.ResourceFormInsert	ثبت شکل فرآورده
Ordinary	AuditLogAction.PIDSicknessCaseUpdate	ویرایش پرونده PID
Ordinary	AuditLogAction.PIDSicknessCaseInsert	ثبت پرونده PID
Ordinary	AuditLogAction.PatientUpdate	ویرایش اطلاعات بیمار
Ordinary	AuditLogAction.PatientPartyUpdate	ویرایش اطلاعات متعامل بیمار
Ordinary	AuditLogAction.PatientPartyInsert	ثبت اطلاعات متعامل بیمار
Ordinary	AuditLogAction.PatientInsert	ثبت اطلاعات بیمار
Ordinary	AuditLogAction.OTPCodeAccepted	کد OTP تایید شد
Ordinary	AuditLogAction.OtismSicknessCaseUpdate	ویرایش پرونده اوتیسم
Ordinary	AuditLogAction.OtismSicknessCaseInsert	ثبت پرونده اوتیسم
Ordinary	AuditLogAction.organizationalPartyUpdate	ویرایش متعامل سازمانی حوزه سلامت
Ordinary	AuditLogAction.organizationalPartyInsert	ثبت متعامل سازمانی حوزه سلامت
Ordinary	AuditLogAction.MSSicknessCaseUpdate	ویرایش پرونده ام اس
Ordinary	AuditLogAction.MSSicknessCaseInsert	ثبت پرونده ام اس
Ordinary	AuditLogAction.MPSicknessCaseUpdate	ویرایش پرونده MPS
Ordinary	AuditLogAction.MPSicknessCaseInsert	ثبت پرونده MPS

Ordinary	AuditLogAction.MetabolicOtherSicknessCaseUpdate	ویرایش پرونده سایر بیماری های متابولیک
Ordinary	AuditLogAction.MetabolicOtherSicknessCaseInsert	ثبت پرونده سایر بیماری های متابولیک
Ordinary	AuditLogAction.LicenseTrustedDoctorOpinionStatusUpdate	ویرایش نظر پزشک معتمد - مجوز
Ordinary	AuditLogAction.LicenseTrustedDoctorOpinionStatusInsert	ثبت نظر پزشک معتمد - مجوز
Ordinary	AuditLogAction.JsonSicknessCaseLicenseUpdate	ویرایش مجوز پرونده
Ordinary	AuditLogAction.JsonSicknessCaseLicenseInsert	ثبت مجوز پرونده
Ordinary	AuditLogAction.HaemophiliaSicknessCaseUpdate	ویرایش پرونده هموفیلی
Ordinary	AuditLogAction.HaemophiliaSicknessCaseInsert	ثبت پرونده هموفیلی
Ordinary	AuditLogAction.HaemophiliaSicknessCaseDelete	حذف پرونده هموفیلی
Ordinary	AuditLogAction.HaemophiliaCenterPartyInsert	ثبت متعامل مرکز هموفیلی
Ordinary	AuditLogAction.GenericResourceCategoryUpdate	ویرایش گروه ژنریک
Ordinary	AuditLogAction.GenericResourceCategoryInsert	ثبت گروه ژنریک
Ordinary	AuditLogAction.EbSicknessCaseUpdate	ویرایش پرونده EB
Ordinary	AuditLogAction.EbSicknessCaseInsert	ثبت پرونده EB
Ordinary	AuditLogAction.DrugUsageInformationUpdate	ویرایش نحوه مصرف دارو
Ordinary	AuditLogAction.DrugUsageInformationInsert	ثبت نحوه مصرف دارو
Ordinary	AuditLogAction.DoctorInfoUpdate	ویرایش اطلاعات پزشک
Ordinary	AuditLogAction.DoctorInfoInsert	ثبت اطلاعات پزشک
Ordinary	AuditLogAction.DiabetSicknessCaseUpdate	ویرایش پرونده دیابت
Ordinary	AuditLogAction.DiabetSicknessCaseInsert	ثبت پرونده دیابت
Ordinary	AuditLogAction.CreateOTPCode	ایجاد کد OTP برای کاربر
Ordinary	AuditLogAction.UserLoginWithOTP	ورود کاربر به سامانه با OTP
Ordinary	AuditLogAction.UserLogin	ورود کاربر به سامانه

- در محصول امکان حذف غیرمجاز داده ممیزی وجود 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 از جدول مربوطه در نظر گرفته شده است، این فیلدها کنار هم قرار داده شده و به آنها یک مقدار عددی رندم بعنوان salt اضافه شود و سپس با الگوریتم SHA256 هش گرفته شود و مقدار هش در یک ستون جدید در جدول رکوردهای ممیزی نگهداری شود.

سپس هر بار که واسط رویدادهای سیستم مشاهده می شود، بررسی صحت داده ها صورت می گیرد. نام جدول و فیلدهایی که هش براساس آنها ایجاد می شود در ادامه آورده شده است.

TBL_AUDITLOG

(CLIENTIP, ACTIONNAME, ACTIONTYPE, ENTITYID, ENTITYNAME, EVENTRESULT, EVENTTYPE, ISVALID, RECORDDATETIME, TAG, USERID, USERNAME, DESCRIPTION,APPLICATIONID)

در صورت دستکاری یکی از فیلدهای جدول TBL_AUDITLOG از طریق پایگاه داده ، زمانیکه مدیر سامانه از طریق واسط کاربری بخش رویدادهای سیستم را مشاهده نماید، رکورد مرتبطی که نشان میدهد کدام رکورد از کدام جدول دستکاری شده است ثبت خواهد شد.

تنظیمات حدآستانه تعداد رکوردهای رویدادهای ممیزی انجام می شود. در صورت رسیدن به مقدار حدآستانه تنظیم شده ، اطلاع رسانی به مدیر سیستم بصورت پیش فرض هر روز ساعت ۸ صبح صورت می گیرد.

تنظیمات مربوطه از طریق فایل webconfig پارامتر NotifyOnOutOfMaxAuditStartTimeStr صورت می گیرد و می توان زمان اطلاع رسانی رسیدن به حدآستانه را به مدیر سیستم را تغییر داد. فرآیند به اینصورت است که راس ساعت تعیین شده تعداد رویداد های ثبت شده را بررسی می کند اگر مقدار آن از حد آستانه بیشتر باشد اقدام به ارسال پیامک(در صورت فعال بودن در تنظیمات امنیتی) می کند و رکورد لاگ مرتبط آن را ثبت خواهد شد. لازم به ذکر است سامانه به صورت اتوماتیک تمامی کاربران با نقش ادمین را جستجو کرده و برای هر کدام یک پیامک ارسال خواهد کرد و این مورد هر روز راس ساعت تعیین شده تکرار میگردد. عملیات بازنویسی روی رکوردهای قدیمی به این صورت می باشد که مقدار حد آستانه را از بخش تنظیمات امنیتی دریافت کرده و با ۲۰٪ تعداد رکورد تنظیم شده جمع میکند و اگر تعداد رویداد های ثبت شده از این عدد بیشتر باشد سامانه اقدام به حذف رویداد های قدیمی ثبت شده میکند و این مکانیزم هر ۱۵ دقیقه یکبار انجام میشود، لازم به ذکر است تعداد رویداد های باقیمانده پس از عمل حذف برابر با (حدآستانه + ۲۰٪) میباشد. (FAU_STG.1.1, FAU_STG.1.2, FAU_STG.3.1, FAU_STG.4.1)

کلاس عملیات رمزنگاری

- محصول برای بررسی صحت داده های ممیزی و رمزنگاری پسورد کاربران از الگوریتم رمزنگاری SHA256 استفاده می نماید. طول کلید ۲۵۶ بایت می باشد. (FCS_COP.1.1(1), FCS_COP.1.1(2))
کد تشخیص صحت داده:

```
public static string CreateChecksum(AuditLog auditLog)
{
    return CryptoHelper.ComputeHash(getPlainChecksum(auditLog));
}

public static bool IsValidChecksum(AuditLog auditLog)
{
    var isvalid = CryptoHelper.VerifyHash(getPlainChecksum(auditLog), "SHA256", auditLog.CheckSum
?? "");
    return isvalid;
}

private static string getPlainChecksum(AuditLog auditLog)
{
    return $"{auditLog.ClientIP}" +
        $"{auditLog.ActionName}" +
        $"{auditLog.ActionType}" +
        $"{auditLog.EntityID}" +
        $"{auditLog.EntityName}" +
        $"{auditLog.EventResult}" +
        $"{auditLog.EventType}" +
        $"{auditLog.IsValid}" +
        $"{auditLog.RecordDateTime}" +
        $"{auditLog.Tag}" +
```

```
    "${auditLog.UserID}" +  
    "${auditLog.UserName}" +  
    "${auditLog.Description}" +  
    "${auditLog.ApplicationID}";  
}
```

- 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.1.3 و FCS_TLSC.1.2)
- محصول از مجموعه رمز ECDHE در برقراری ارتباط با سرور خارجی پشتیبانی نمی کند.
(FCS_TLSC_EXT.4.1)

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. در صورت تنظیم تعداد تلاش های ناموفق برابر با n در N+1 امین تلاش ناموفق حساب کاربری 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 احراز هویت (رمز عبور و نام کاربری)
 - نقش کاربر
 - وضعیت حساب کاربری (فعال، غیرفعال، مسدود)
- محصول امکان مدیریت پیچیدگی رمز عبور و طول آن را دارد. این امکان توسط مدیرسامانه قابل تنظیم است. (FIA_PMG_EXT.1.1)
- کاربران می توانند قبل از احراز هویت به لینک های زیر دسترسی داشته باشند:
 - ارائه لیست مراکز درمانی دیابت
 - لیست بیماریهای نادر در اولویت واکسیناسیون
 - ارائه لینکی به بیماران دیابتی که می‌توانند از آن برای اطمینان از ثبت کدملی و صحت اطلاعات خود استفاده کنند.

- بارگذاری جواب آزمایش ژنتیک بیماران متابولیک
- همچنین امکان استفاده و دانلود فایل‌های آموزشی که بعد از احراز هویت در دسترس هستند، بدون احراز هویت نیز وجود دارد. (FIA_UID.1.2 ، FIA_UID.1.1 ، FIA_UAU.1.2،FIA_UAU.1.1)
- سامانه امکان احراز هویت دو عاملی با نام کاربری و رمزعبور و ارسال کد امنیتی به شماره همراه کاربر را دارد. (FIA_UAU.5.2، FIA_UAU.5.1)
- 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.1.3 ، FIA_USB.1.2 ، FIA_USB.1.1)
- محصول تنها در صورت دریافت گواهی معتبر از سرور خارجی، اجازه برقراری ارتباط را می‌دهد. (FIA_X509_EXT.2.1 ، FIA_X509_EXT.1.2 ، FIA_X509_EXT.1.1)
- در صورتیکه محصول قادر به برقراری ارتباط جهت اعتبارسنجی گواهی دیجیتال نباشد و یا به هر دلیلی نتواند لیست cfl را چک کند، گواهی را نمی‌پذیرد و از برقراری ارتباط جلوگیری خواهد کرد. (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 فعال و غیرفعال در سیستم 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.1.4 ، FDP_ACF.1.3 ، FDP_ACF.1.2 ، FDP_ACF.1.1)
- محصول تضمین می‌نماید در زمان آزادسازی منابع اطلاعات آنها به طور کامل حذف خواهد گردید. لازم به ذکر است، با توجه به اینکه از نام کاربری در سند های "پرونده ها" مختلف استفاده شده و نیاز به این مورد که چه کاربری چه فعالیت هایی در سامانه داشته، حتی پس از حذف کاربر، امکان انتساب نام کاربری به کاربر دیگر مقدور نمی‌باشد (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_INFO

(APPID , AUTHENTICATIONTYPE ,EMAIL, FIRSTNAME, GENDER, LASTNAME, MOBILENO, NATIONALCODE, ORGN_ID, TAG1, TEL, USERNAME,TAG2,TAG3, TAG4,TAG5,TAG9, TAG10)

در صورت دستکاری یکی از فیلدهای جدول بالا از طریق پایگاه داده، زمانیکه کاربر بخواهد وارد سامانه شود جلوی آن گرفته خواهد شد. همچنین پس از لاگین ناموفق کاربر رکورد لاگی با عنوان "تغییر غیر مجاز اطلاعات کاربر" در بخش رویدادهای ممیزی جهت مطلع سازی مدیر سامانه ثبت خواهد شد.

TBL_JSON_SICKCASE

(AUTHOR_IXID, AUHTOR_TYPE, AUTHOR_IXID, AUHTOR_TYPE, DOCTOR_COUNCIL_CODE, DOCTOR_INFO_ID, DOCTOR_SPECIALITY_ID, DOCUMENT_NUMBER, DOCUMENT_TRACKING_CODE, FIRST_VACCINATION_DATE, HEALTH_CENTER_NAME, HEALTH_CENTER_IXID, HEALTH_CENTER_TYPE, INSURANCE_EXPIRE_DATE, INSURER_ID, INSURER_NAME, INSURANCE_NO, MEDICINE_DELIVERY_ADDRESS, PATIENT_BIRTHDATE, PATIENT_CITY_ID, PATIENT_CITY_NAME, PATIENT_FATHER, PATIENT_FNAME, PATIENT_COUNTRY_ID, PATIENT_COUNTRY_CODE, PATIENT_GENDER, PATIENT_ID, PATIENT_LNAME, PATIENT_MOBILE_NO, PATIENT_NATIONAL_CODE, PATIENT_SICKNESS_ID, RECEIVER_IXPARTYID, RECEIVER_PARTYIDENTITY_TYPE, RECEIVER_PARTY_NAME, RECEIVER_PARTY_TYPE, SENDER_IXPARTYID, SENDER_PARTYIDENTITY_TYPE, SENDER_PARTY_NAME, SENDER_PARTY_TYPE, SICKCASE_TYPE_ID, SICKNESS_DATE, SUBMIT_DATE, SICKNESS_TYPE_NAME, SICKNESS_TYPE_ID)

در صورت دستکاری یکی از فیلدهای جدول بالا از طریق پایگاه داده، زمانیکه کاربر مربوطه بخواهد از طریق بخش پرونده < مشاهده > مجوزها را بررسی کنید، پیغام " شناسایی تغییر غیر مجاز پرونده بیمار" نمایش داده می شود و همینطور لاگ مرتبطی جهت مطلع سازی مدیر سامانه با عنوان "تغییر غیر مجاز اطلاعات پرونده" ثبت خواهد شد. همچنین اگر کاربر مجاز از طریق منوی اسناد < پرونده بیمار > مجوزهای تحویل فرآورده، مجوزها را مشاهده نماید، این بررسی صورت خواهد گرفت و لاگ مرتبط جهت اطلاع رسانی به مدیر ثبت می شود.

(FDP_SDI.2.2,FDP_SDI.2.1)

کلاس مدیریت امنیت

- محصول امکان فعال و غیرفعال نمودن کارکردهای تنظیمات امنیتی سامانه توسط مدیرسامانه را دارد. این کارکردها شامل ثبت انواع سطح 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 مشخصه های امنیتی مانند تلاش ناموفق برای ورود از مقادیر پیش فرض استفاده می نماید. این مقادیر قابل تغییر توسط مدیرسامانه هستند. (FMT_MSA.3.2, FMT_MSA.3.1, FMT_MSA.1.1)
- محصول قابلیت اختصاص و یا حذف نقش های موجود در سامانه به کاربران، پرس و جو روی رویدادهای ممیزی سیستم ، تغییر در داده های کاربران توسط مدیرسامانه را دارد. در صورت اعطای دسترسی توسط مدیر سامانه روی بخش (تنظیمات- تغییر رمز عبور)، کاربر عادی نیز امکان تغییر رمز عبور خود را دارد. (FMT_MTD.1.1 (1), FMT_MTD.1.1 (2))
- محصول قادر است کارکردهای امنیتی زیر را اعمال نماید. (FMT_SMF.1.1)

- کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
- پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
- پشتیبانی از حد آستانه
- مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
- ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
- مدیریت حدآستانه برای تلاش ناموفق احراز هویت
- مدیریت پیچیدگی رمز عبور
- امکان مدیریت ایجاد محدودیت در احراز هویت
- امکان مدیریت نقش ها و دسترسی های کاربران
- امکان تعیین مدت زمان خاتمه نشست غیرفعال
- محصول دارای نقش‌های مدیرسامانه، کاربر عادی 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 فعالیت جاری را متوقف می کند. (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 سامانه تنظیم می‌شود. کلیه نشست های فعال محصول پس از مدت زمان تعیین شده توسط مدیر سامانه خاتمه خواهند یافت، توجه شود این تنظیمات برای کاربرانی که پس از تنظیم زمان خاتمه نشست، وارد سامانه شده اند اعمال می شود. کاربران سامانه از طریق دکمه خروج در تمامی صفحات سامانه امکان خاتمه دادن به نشست خود را دارند. (FTA_SSL.4.1, FTA_SSL.3.1, FTA_MCS.1.2, FTA_MCS.1.1)

- محصول قادر است پس از برقراری نشست موفقیت‌آمیز تلاش‌های ناموفق برقراری نشست را با نمایش روز و ساعت، و تعداد تلاش ناموفق را به کاربران نمایش دهد، این اطلاعات از گوشه سمت چپ بالای صفحه آیکون ا در دسترس است. این اطلاعات جهت مشاهده کاربران در اختیار آنها قرار می‌گیرد. محصول امکان ایجاد محدودیت جهت برقرار نشست براساس IP، شناسه کاربری، نقش و محدوده زمانی را دارد.
(FTA_TSE.1.1, FTA_TAH.1.3, FTA_TAH.1.2, FTA_TAH.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 در حال تبادل حفاظت نماید. این امکان برای مدیر سیستم نیز مهیا و الزامی است. (FTP_TRP.1.3, FTP_TRP.1.2, FTP_TRP.1.1)
- محصول از پروتکل امن ارتباطی TLS جهت ارتباط خود با سرور پیام کوتاه استفاده می‌نماید. محصول از ارسال پیام کوتاه برای ارسال هشدار حد آستانه و احراز هویت دو مرحله‌ای استفاده می‌کند.
(FTP_ITC.1.3, FTP_ITC.1.2, FTP_ITC.1.1)

۷- توجیحات

الزامات زیر برای محصول کاربرد ندارند:

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 ها برای سامانه کاربردی ندارد.

- مولفه های 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 مولفه ها در محصول تحت وب کاربرد ندارد.