به نام خدا

سند هدف امنیتی سیستم مالی اداری شرکت نمادایران نسخه ۴,۱,۰,۰

شرکت نمادایران

اردیبهشت ۱۴۰۲

نسخه ۶,۰

فهرست

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سندهدف امنیتی	سند هدف امنیتی سیستم مالی اداری نمادایران
نسخه	۶
تاریخ	۱۴۰۲/۰۲
نویسندگان	شرکت نمادایران

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت نمادایران
نام محصول	نرم افزار مالی اداری
نوع محصول	نرم افزار کاربردی تحت شبکه(ویندوزی)
نسخه	۴.۱.۰.۰

۱-۳- مرور کلی هدف ارزیابی

- ممیزی امنیت
- درهم سازی / رمزنگاری
- احراز هویت
- مدیریت امنیت
- کنترل دسترسی
- کانالها/مسیرهای مورد اعتماد
- کنترل گردش مستندات و اطلاعات

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

۱-۳-۲- نوع هدف ارزیابی

نرم افزار مالی اداری نمادایران،نرم افزار کاربردی تحت ویندوز ا ست که معماری آن کلاینت سروری بوده و در نتیجه منطبق با پروفایلهای حفاظتی زیر میباشد :

- برنامه های کاربردی تحت شبکه
- برنامه کاربردی

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

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

کامپوننت‌ها	حداقل الزامات
سیستم عامل	Window 10
RAM	۲ □□ □□ □□□□□□
H.D.D	۲۰ □□ □□ □□□□□□
Network	۱۰۰ □□□□

۴-۱- توصیف هدف ارزیابی

۱-۴-۱- حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
قفل سخت افزاری	محصول شرکت الکترونیکی بردهای هوشمند

۲-۴-۱- حوزه منطقی

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

کارکردها	توصیف
احراز هویت	بوسیله نام کاربری و رمز عبور و احراز هویت دوعامله
مدیریت امنیت	بوسیله برنامه مجوزدهی به هر کاربر یا گروه کاربری
ممیزی	ثبت ممیزی موارد ذکر شده در الزامات امنیتی و همچنین عملیات مهم کاربران در سطح هر سیستم اطلاعاتی شرکت نماد ایران
درهم سازی/رمز نمودن داده	داده های حساس کاربر طبق الزامات و الگوریتم های ذکر شده امنیتی بصورت محرمانه نگهداری میشوند.
کانالها/مسیرهای مورد اعتماد	مسیر ارتباطی امن بین کاربران و پایگاه داده با استفاده از پروتکل TLS
کنترل دسترسی	محصول قابلیتهای لازم برای محدود کردن دسترسی را دارد، به طوری که تنها موجودیتهای مجاز به داده و کارکردهای محصول دسترسی دارند.
کنترل گردش مستندات و اطلاعات	حداکثر اندازه فایل میتواند به صورت پویا برای هر نوع سند تعریف شود.همچنین تنها کاربران مجاز،مجوز صدور و ارسال هر رکورد را دارند.
حفاظت از داده ها	محصول به هیچگونه منبعی (نرم افزاری و سخت افزاری) دسترسی ندارد و تنها با ارتباط امن به شبکه متصل 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 (اسفند ۹۶ نسخه ۱) - برنامه کاربردی(مهر۹۵ نسخه ۱)

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	EAL 1

۳- تعریف مسائل امنیتی

۳-۱- خطمشی

خطمشی	توصیف
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار میگیرند.
پیکربندی مناسب	پیکربندی پیشفرض محصول و مؤلفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوری که 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 rootپیشفرض، خطاهای پیشفرض و صفحات ۴۰۴ ،مقادیر احراز هویت پیشفرض، نام کاربری پیشفرض، پورتهای پیشفرض، صفحات پیشفرض که اطلاعات داخلی همچون شماره نسخه را آشکار مینمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانی که محصول یا هر مؤلفه تعاملی به طور گسترده مورد استفاده قرار میگیرد؛ بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی میتوان از حمله مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳-۲- تهدیدات

تهدید	توصیف
دسترسی غیرمجاز	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 نقصهای 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 داده های میتوانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به داده ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و داده های 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 داده های 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.

تهدید	توصیف
انکار	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.
افشای اطلاعات	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 عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	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.
داده های ورودی مخرب	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.
سطح دسترسی بالاتر	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.
شنود شبکه	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، اطالعات محرمانه خود را وارد میکند.
T.NETWORK_ATTACK	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار میگیرد. مهاجمان ممکن است سعی در برقراری ارتباط با برنامه کاربردی نمایند یا در ارتباطات میان نرم افزار برنامه کاربردی و دیگر نقاط پایانی دست ببرند تا بتوانند به آن نفوذ کنند
T.NETWORK_EAVESDROP	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار میگیرد. مهاجمان ممکن است داده های انتقالی بین برنامه کاربردی و دیگر نقاط پایانی را مشاهده کنند یا به آنها دسترسی یابند.
T.LOCAL_ATTACK	فرد مهاجم ممکن است از طریق نرم افزارهای عادی (نرم افزارهایی که امتیاز دسترسی ویژه ندارند) موجود روی پلتفرمی که برنامه کاربردی روی آن اجرا میشود، وارد عمل شود. مهاجمان ممکن است ورودیهای آلوده را در قالب فایل یا ارتباطات محلی، وارد برنامه کاربردی کنند.
T.PHYSICAL_ACCESS	مهاجم ممکن است به اطلاعات حساس بایگانی شده، دسترسی پیدا کند.

۳-۳- فرضیات

فرضیه	توصیف
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال می نمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال مینمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیریهای شناخته شده را اتخاذ می نمایند.
محیط امن	فرض شده است که تمام پیش بینیهای محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیرقانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت میگیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مؤلفه های سخت افزاری دارای پشتیبان مناسبی هستند و بنا بر وجود نسخه پشتیبان هیچ داده ای از دست نمیرود. همچنین به علت شکست در سیستم، قطع سرویسی رخ نمیدهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانالهای ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت میشوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ میشود.
A.PLATFORM	اجرای محصول منوط به یک پلتفرم رایانشی قابل اعتماد است و شامل پلتفرم زیرین و هرگونه محیط زمان اجرا که پلت فرم برای محصول فراهم کرده است.
A.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمیزند و نرم افزار را در تبعیت از سیاستهای امنیتی سازمانی که از آن استفاده میکند، به کار میگیرد.
A.PROPER_ADMIN	راهبر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمیزند، بی دقت نیست و نرم افزار را در تبعیت از سیاستهای امنیتی سازمانی که از آن استفاده میکند، راهبری مینماید.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد کند. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت کند. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه کند.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت کند و مطابق با نقش و مجوزهایشان مجاز کند. محصول باید برای احراز هویت کاربر، قوانینی تعریف کند طوری که کاربران را ملزم به استفاده از کلمه های عبور قدرتمند کند. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف کند. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم میکند. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم کند. 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 کند. از جمله سازوکارها میتوان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت بر اساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده های غیرمجاز را کنترل و مدیریت کند. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنج IPتعریف شده میتواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم کند که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده کند.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل کند و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارآمد سیستم فراهم کند. 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 کند.
مدیریت خطا	محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم کند. 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 کند.
مدیریت داده های باقیمانده	محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس میگردد
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLSاستفاده نمایند.
O.INTEGIRITY	محصوولات انطباق پذیر، صحت نصب خود و بسته های به روزرسانی را تضمین میکنند و همچنین اقدامات اجرایی محیط محور را در جهت کاهش تهدیدات، تسهیل مینمایند. نرم افزارهای خیلی کمی، اگر نگوییم هیچ، عاری از خطا هستند؛ بنابراین، توانایی نصب بسته های تعمیر و عیب یابی و به روزرسانی نرم افزارهای نصب شده به صورت منسجم، اقدامی ضروری برای امنیت شبکه های سازمانی است.سازندگان پردازشگرها،برنامه نویسان کامپایلر، فروشندگان محیطهای اجرا و فروشندگان سیستم عاملها، اقدامات اجرایی محیط محوری را در جهت کاهش تهدیدات ایجاد کرده اند که با پیچیده تر کردن وظایف سیستمها، کار نفوذ به آنها را برای مهاجمان، دشوارتر و پرهزینه تر میکند. نرم افزارهای برنامه کاربردی اغلب میتوانند از این سازوکارها بهره ببرند.این کار با اسوتفاده از API هایی انجام میشود که در زمان اجرا فراهم شده است؛ یا توسط فعالسازی این سازوکارها از طریق کامپایلر یا لینکر
O.QUALITY	برای تضمین کیفیت پیاده سازی، محصولات انطباق پذیر به جای پیاده سازی سرویسها و API های خود،سرویسهاو API هایی را به کار میگیرند که توسط محیط زمان اجرا تأمین شده است.اهمیت این کار به طور خاص برای سرویسهای رمزنگاری و دیگر عملیات پیچیده ای مثل تجزیه فایل و رسانه، بیشتر است.بهره گیری از این قابلیت پلتفرم، فقط منوط به استفاده از API های هستند و پشتیبانی شده است.
O.MANAGEMENT	برای تسهیل روند مدیریت توسط کاربران و سازمان، محصولات انطباق پذیر، واسطهای منسجم و پشتیبانی شده ای را برای نگهداری و پیکربندی امنیتی خود فراهم میکنند. این کار شامل پیاده سازی و به روزرسانی برنامه کاربردی با استفاده از قالبها و سازوکار پیاده سازی پشتیبانی شده توسط پلتفرم و همچنین فراهم کردن سازوکاری برای پیکربندی است.
O.PROTECTED_STORAGE	برای جلوگیری از افشای اطلاعات محرمانه ی کاربر در نتیجه ی حوادثی که منجر به از دست رفتن کنترل فیزیکی ابزارهای ذخیره سازی میشوند، محصولات انطباق پذیر از شیوه های حفاظت داده های بایگانی شده استفاده میکنند. این کار شامل رمزگذاری داده ها و ذخیره کلیدها توسط محصول است تا از دسترسی غیرمجاز به این داده ها جلوگیری شود.

O.PROTECTED_COMMS	برای جلوگیری از حملات تهدیدآمیز فعال (دستکاری بسته های داده) و غیرفعال (استراق سمع)، محصولات انطباق پذیر از یک کانال مورد اعتماد برای انتقال داده های حساس استفاده میکنند. داده های حساس شامل کلیدهای رمزنگاری، گذرواژه ها وهرگونه داده های دیگری است که مربوط به برنامه کاربردی بوده و نباید خارج از برنامه کاربردی، در معرض دید باشند.

۲-۴- اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مؤلفه ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفه های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی میتوان به غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله های لازم برای تمام آسیب پذیریهای امنیتی شناخته شده را در نظر میگیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه های غیر از محصول نیز مورد ممیزی قرار میگیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول است. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور آزمون باید پاک یا غیرقابل دسترس گردند.
پشتیبان گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده های باقیمانده در محیط عملیاتی محصول را حفظ کند.برای این منظور ممکن است از روالهای از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مؤلفه های سخت افزاری نیز نسخه پشتیبان تهیه گردد.
OE.PLATFORM	اجرای محصول متکی به یک پلتفرم رایانشی مورد اعتماد است. این شامل سیستم عامل زیرین و هرگونه محیط اجرایی دیگری نیز میشود که در اختیار محصول قرارگرفته است.

هدف امنیتی	توصیف
OE.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمیزند و نرم افزار را در تبعیت از سیاستهای امنیتی سازمانی که از آن استفاده میکند، به کار میگیرد.
OE.PROPER_ADMIN	راهبر برنامه کاربردی بی دقت نیست و از روی عمد دست به اشتباه یا خرابکاری نمیزند و نرم افزار را در تبعیت از سیاستهای امنیتی سازمانی که از آن استفاده میکند، راهبری مینماید.

۵- نیازمندی‌های امنیتی

❖ توضیحات : در متن الزامات زیر نوتاسیون انتخاب بصورت زیرخط دار و نوتاسیون اختصاص بصورت بولد نمایش داده شده است.

۵-۱- الزامات کارکردامنیتی برنامه های کاربردی تحت شبکه

الزامات کارکردامنیتی زیر مطابق پروفایل حفاظتی برنامه های کاربردی تحت شبکه تهیه شده‌اند.

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱	ممیزی امنیت	تولید داده ممیزی ۱	FAU_GEN.1.1
۲		تولید داده ممیزی ۲	FAU_GEN.1.2
۳		مرتبط نمودن هویت کاربر به رویداد ۱	FAU_GEN.2.1
۴		بازبینی داده ممیزی ۱	FAU_SAR.1.1
۵		بازبینی داده ممیزی ۲	FAU_SAR.1.۲
۶		بازبینی داده ممیزی محدود۱	FAU_SAR.2.1
۷		بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.3.1
۸		انتخاب داده ممیزی ۱	FAU_SEL.1.1
۹		ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۱۰		ذخیره سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۱۱		اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1
۱۲		پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱	FAU_STG.4.1

۱۳	**عملیات رمزنگاری**	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۴		عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(۲)
۱۵	**حفاظت از داده کاربر**	خط مشی کنترل دسترسی ۱	FDP_ACC.1.1
۱۶		عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۱۷		عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۱۸		عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۱۹		عملیات کنترل دسترسی ۴	FDP_ACF.1.4
۲۰		حفاظت کامل از اطلاعات باقیمانده در منابع	FDP_RIP.2.1
۲۱			
۲۲			
۲۳			
۲۴			
۲۵			
۲۶			
۲۷	**حفاظت از داده کاربر**	صحت داده کاربری ذخیره شده۲	FDP_SDI.2.1
۲۸		صحت داده کاربری ذخیره شده۳	FDP_SDI.2.2
۲۹	**شناسایی و احراز هویت**	مدیریت احرازهویت ناموفق۱	FIA_AFL.1.1
۳۰		مدیریت احرازهویت ناموفق۲	FIA_AFL.1.2
۳۱		تعریف مشخصات کاربر۱	FIA_ATD.1.1
۳۲		مدیریت کلمه عبور	FIA_PMG_EXT.1.1

۳۳		احرازهویت کاربر۱	FIA_UID.1.1
۳۴		احرازهویت کاربر۲	FIA_UID.1.2
۳۵		سازوکار احرازهویت چندگانه۱	FIA_UAU.5.1
۳۶		سازوکار احرازهویت چندگانه۲	FIA_UAU.5.2
۳۷		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۱	FIA_USB.1.1
۳۸		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۳۹		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۳	FIA_USB.1.3
۴۰	**مدیریت امنیت**	مدیریت کارکرد در محصول۱	FMT_MOF.1.1
۴۱		مدیریت مشخصه های امنیتی۱	FMT_MSA.1.1
۴۲		مدیریت مشخصه های امنیتی ۳	FMT_MSA.3.1
۴۳		مدیریت مشخصه های امنیتی ۴	FMT_MSA.3.2
۴۴		مدیریت داده‌های محصول ۱ – مدیر سیستم	FMT_MTD.1.1 (1)
۴۵		مدیریت داده‌های محصول ۱ – کاربر عادی، وارد کننده داده	FMT_MTD.1.1 (2)
۴۶		کارکردهای مدیریتی محصول۱	FMT_SMF.1.1
۴۷		نقشهای امنیتی ۱	FMT_SMR.1.1
۴۸		نقشهای امنیتی ۲	FMT_SMR.1.2
۴۹	**حفاظت از داده توابع امنیتی هدف ارزیابی**	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۵۰		انتقال داده امنیتی در داخل محصول۱	FPT_ITT.1.1
۵۱		سازگاری داده امنیتی بین محصول و موجودیت امن۱	FPT_TDC.1.1

۵۲		مهرهای زمانی۱	FPT_STM.1.1
۵۳		به روزرسانی امن۲	FPT_TUD_EXT.1.2
۵۴		به روزرسانی امن۳	FPT_TUD_EXT.1.3
۵۵	**تخصیص منابع**	تحمل خطا۱	FRU_FLT.1.1
۵۶	**دسترسی به محصول**	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۷		محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
۵۸		خاتمه دادن به نشستها توسط محصول۱	FTA_SSL.3.1
۵۹		خاتمه دادن به نشستها توسط کاربر۱	FTA_SSL.4.1
۶۰		سوابق دسترسی به محصول۱	FTA_TAH.1.1
۶۱		سوابق دسترسی به محصول۲	FTA_TAH.1.2
۶۲		سوابق دسترسی به محصول۳	FTA_TAH.1.3
۶۳		برقراری نشست۱	FTA_TSE.1.1
۶۴	**کانال‌ها و مسیرهای امن**		
۶۵			
۶۶			
۶۷		کانال امن ۱	FTP_ITC.1.1
۶۸		کانال امن ۲	FTP_ITC.1.2
۶۹		کانال امن ۳	FTP_ITC.1.3

۷۰	**عملیات رمزنگاری**	تخریب کلید رمزنگاری ۱	FCS_CKM.4.1
۷۱		عملیات رمزنگاری -۱رمزنگاری و رمزگشای ۱ (۳)	FCS_COP.1.1(3)
۷۲		الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۷۳		الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۷۴		الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۷۵			
۷۶			
۷۷		الزامات پروتکل TLS Client(۱)	FCS_TLSC_EXT.1
۷۸			
۷۹	**شناسایی و احراز هویت**	الزامات پروتکل X509(۱)ابطال	FIA_X509_EXT.1.1/Rev
۸۰		الزامات پروتکل X509(۱)ابطال	FIA_X509_EXT.1.2/Rev
۸۱		الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1

الزامات کارکرد امنیتی برنامه کاربردی تحت شبکه

۱-۱-۵- کلاس ممیزی امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_GEN.۱	- FPT_STM.1	۱	FAU_GEN.1.1	محصول بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید میکند: • آغاز و اتمام توابع ممیزی • تمامی رویدادهای قابل ممیزی (برای نوع داده حســـاس و داده هایی که بار حقوقی دارند) که در جدول یک آمده است.
		۱	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 دا شته باشد) و نتیجه (موفقیت یا شکست) رویداد • **نام دستگاه کاربر،نام کاربری ویندوز**
FAU_GEN.۲	- FAU_GEN.1 - FIA_UID.1	۲	FAU_GEN.2.1	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 کند.
FAU_SAR.۱	- FAU_GEN.1	۳	FAU_SAR.1.1	محصول باید امکان خواندن **کلیه‌ی رویدادهای ممیزی** را برای **کاربران یا گروه‌های کاربری مجاز** فراهم نماید.
		۴	FAU_SAR.1.2	محصـــول باید رکوردهای ممیزی را طوری فراهم میکند که کاربر بتواند آنها را درک و اطلاعات این رکوردها را تفسیر کند.
FAU_SAR.۲	- FAU_SAR.1	۵	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.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_SAR.۳	- FAU_SAR.1	۶	FAU_SAR.3.1	محصول امکان انجام **متدهای انتخاب و مرتب سازی** رکوردهای ممیزی را به نحوی فراهم کند که کاربر مجاز بتواند آن رکوردها را براساس **تمام اطلاعات قابل نمایش مانند کد و نام کاربر،تاریخ/زمان، نام دستگاه، نوع رخداد** مرتب کند.
FAU_SEL.1	- FAU_GEN.1 - FMT_MTD.1	۷	FAU_SEL.1.1	توابع امنیتی هدف ارزیابی باید قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شـــدن،از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه‌های زیر باشد: • نوع رخداد • **تنها رخدادهای ممیزی کم‌اهمیت باید برای عدم ثبت در فایل‌های ممیزی انتخاب شوند**
FAU_STG.۱	- FAU_GEN.1	۸	FAU_STG.1.1	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را، از حذف غیرمجاز حفاظت کند.
		۹	FAU_STG.1.2	محصول قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره سازی آنها هست.
FAU_STG.۳	- FAU_STG.1	۱۰	FAU_STG.3.1	محصول در صورت تجاوز دنباله ممیزی از **محدوده حجم قابل تنظیم** باید با استفاده از **ایمیل یا پیام کوتاه،یک پیغام در گردش کار،از طریق واسطهای محصول کاربران مربوطه را** مطلع میکند.
FAU_STG.۴	- FAU_STG.1	۱۱	FAU_STG.4.1	محصول در صورت پر شدن دنباله ممیزی، باید رویدادهای ممیزی را نادیده بگیرد و به **تعداد x رکورد(طبق تنظیم تعداد رکورد حذف از لاگ) از ابتدای جدول لاگ،رکورد ها را حذف میکند.**

جدول یک - لیست رویدادهای قابل ممیزی

مؤلفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد۱	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می افتد در حالی که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
اقدامات لازم در زمان از دست رفتن داده ممیزی۱	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
پیشگیری از اتلاف و از بین رفتن داده های ممیزی ۱	عملیات انجام شده به دلیل شکست ذخیره سازی ممیزی (پایه)	
صحت داده های کاربری ذخیره شده ۲	تلاشهای موفقیت آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاشها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
احراز هویت کاربر	ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
سازوکار احرازهویت چندگانه	ثبت نتایج احرازهویت (حداقل) ثبت هر سازوکاراحرازهویت فعال همراه با نتیجه نهائی(پایه)	
شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبدأ، شناسایی نقطه پایانی اتصال
مدیریت کلمه عبور	ثبت رد هر کلمه عبور آزمون شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر

مؤلفه	رویداد قابل ممیزی	جزئیات
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند ایجاد موجودیت فعال) (حداقل)(شکست و موفقیت انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال) (پایه))	
مدیریت مشخصه های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه های امنیتی (پایه)	
مدیریت داده های محصول ۱- مدیرسیستم	تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود
مدیریت داده های محصول ۱- کاربر عادی،وارد کننده داده	تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردهاواسناد باید ثبت شود.
عملیات رمزنگاری(۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه های موجودیتهای فعال و غیرفعال (پایه)	
عملیات رمزنگاری (۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه های موجودیتهای فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی	درخواستهای موفقیت آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	شناسایی داده های موجودیت غیرفعال
ورود داده های کاربری به محصول با مشخصه امنیتی	ورود داده کاربری موفقیت آمیز، شامل هرگونه مشخصه های امنیتی (حداقل) تمامی تلاشها برای وارد کردن داده های کاربری، شامل هرگونه مشخصه های امنیتی (پایه)	
خروج داده های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات بهطور موفقیت آمیز (حداقل) همه تلاشها برای خارج کردن اطلاعات از محصول (پایه)	

مؤلفه	رویداد قابل ممیزی	جزئیات
مدیریت کارکرد در محصول	تمامی تغییرات در رفتارهای کارکردی محصول	
کارکردهای مدیریتی محصول	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
نقشهای امنیتی	ثبت تغییرات در گروههای کاربری که بخشی از یک نقش است (حداقل)	
سازگاری داده های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از سازوکار سازگاری داده های محصول (حداقل) ثبت استفاده از سازوکار سازگاری داده های محصول (پایه)	
حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)	
تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیتهای در حال قطع شدن محصول که به دلیل شکست است (پایه)	
برقراری نشست	ثبت منع آغاز نشست به دلیل سازوکار آغاز نشست (حداقل) ثبت تمامی تلاشها در آغاز نشست کاربر (پایه)	
محدودیت بر روی چندین نشست همزمان	ثبت رد یک نشست مبتنی بر محدودیت نشستهای همزمان (حداقل)	

مؤلفه	رویداد قابل ممیزی	جزئیات
خاتمه دادن به نشستها	ثبت خاتمه دادن به یک نشست بیکار توسط سازوکار 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)**	محصـــول باید **برای وارســـی صـــحت داده‌های ممیزی و داده‌های رکورد** بر اســـاس یک الگوریتم رمزنگاری مشـــخص **SHA-256** اندازه کلید رمزنگاری **هیچکدام** اجرا شـــود که مطابق با **FIPS 180-2** باشد.
FCS_COP.1(2)	- FDP_ITC.1 - FDP_ITC.2 - FCS_CKM.1	۲	**FCS_COP.1.1(2)**	*محصـــول باید* **برای تولید داده درهم سازی** *بر اســاس مجموعه الگوریتم‌های رمزنگاری مشـخص* SHA و اندازه‌کلید رمزنگاری **۲۵۶** *اجرا شود که مطابق با* **FIPS 180-2** *باشد.*
	-	۳	**FCS_CKM.4.1**	*محصول باید بر اساس متد تخریب کلید رمزنگاری* **ازطریق Dispose شدن متغیر حاوی کلید رمزنگاری** *که بر اساس استاندارد* **هیچ استانداردی** *باشد، کلیدهای رمزنگاری را از بین ببرد.*
	-	۴	**FCS_COP.1.1(3)**	محصول باید **رمزنگاری و رمزگشایی** را مطابق با الگوریتم رمزنگاری متقارن AES- XTS مطابق مستند NIST SP 800- 38E, AES-CBC مطابق سند NIST SP 800- 38A و هیچکدام با اندازه کلید رمزنگاری ۲۵۶ بیتی را انجام دهد.
	-	۵	**FCS_TLSC_EXT.1.۱**	محصول باید TLS 1.2 (RFC5246) را پیاده سازی کند و دیگر نسخه های TLSو SSLرا رد کند. همچنین TLSرا با پشتیبانی از مجموعه های رمز زیر را پیاده سازی کند: TLS_RSA_WITH_AES_128_CBC_SHA256مطابق باRFC 5246
	-	۶	**FCS_TLSC_EXT.1.۲**	محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶از RFC 6125 تائید کند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۷	**FCS_TLSC_EXT.1.۳**	محصول باید کانال امن را فقط در صورت معتبر بودن گواهینامه سرور برقرار سازد. اگر گواهینامه سرور غیرمعتبر به نظر رسید، محصول باید ارتباط را برقرار نسازد،**هیچ اقدام دیگری**

۳-۱-۵- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_AFL.1	- FIA_UAU.1	۱	FIA_AFL.1.1	محصول باید بتواند با استفاده از **یک عدد مثبت**، یک عدد مثبت قابل تنظیم توسط مدیر **اعداد صحیح در بازه‌ی ۱ تا ۲۱۴۷۴۸۳۶۴۷** ، تلاش‌های ناموفق احرازهویت مرتبط با **ورود به سامانه** 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 حساب کاربری شخص را غیر فعال کند را اجرا کند که باعث پیچیده تر کردن عمل احراز هویت مجدد کاربر شود
FIA_ATD.1	- -	۳	FIA_ATD.1.1	محصول باید مشخصه های امنیتی زیر را برای هر کاربر نگهداری نماید: • **شناسه کاربر** • **متد احرازهویت مورد استفاده** • **داده احرازهویت** • **نقش کاربر** • **وضعیت حساب کاربری(فعال، غیرفعال، بلوکه شده و غیره)** • **هیچ مشخصه امنیتی دیگر**
	-	۴	FIA_PMG_EXT.1.1	محصـــول باید قابلیتهای مدیریت کلمه عبور را که در زیر ذکر شـــده اند برای کلمه های عبور مدیریتی فراهم کند: ۱. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص مانند **"@"** ، **"هیچ کاراکتر دیگری"** باشد. ۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم میباشد و ۸ کاراکتر یا بیشتر باشد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_UAU.1	- FIA_UID.1	۵	FIA_UID.1.1	محصول باید پیش از احرازهویت کاربر، اجازه اقدامات میانی زیر را به کاربر دهد: • **هیچ اقدامی** • **تنظیمات بانک داده**
		۶	FIA_UID.1.2	توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی نماید.
FIA_UAU.5	- -	۷	FIA_UAU.5.1	محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد: • نام کاربری و کلمه عبور • **احراز هویت چندگانه**
		۸	FIA_UAU.5.2	محصـول باید هر کاربر متقاضـی احرازهویت را مطابق **کاربران از راه‌دور باید علاوه بر بر سی نام کاربری و کل مه عبور از روش احرازهو یت چ ند گا نه (ماند Dual factor authentication) ا ستفاده کند، ار سال کد تایید به ایمیل یا موبایل کاربر** احرازهویت نماید.
FIA_USB.1	- FIA_ATD.1	۹	FIA_USB.1.1	محصول باید مشخصه های امنیتی زیر را برای کاربر فعال نگهداری کند: • **شناسه کاربر** • **نقشها و یا مجموعه دسترسیهای کاربر به قسمتهای مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت(جزئیات تلاش برای احرازهویت موفق و ناموفق)**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **هیچ مشخصه کاربری دیگری**
		۱۰	FIA_USB.1.2	محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت میکند، اعمال کند: • **زمانی که یک نشست جدید برقرار میشود، اعتبار نشستهای قبلی باید از بین برود.** • **اطلاعات پیشینه احراز هویت باید به روزرسانی گردد.** • **هیچ قانون دیگری برای اتصال اولیه مشخصه ها**
		۱۱	FIA_USB.1.3	محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه های امنیتی کاربر فعال اعمال کند: **هیچ تغییری در طول نشست فعال مجاز نیست هیچ قوانین دیگری حاکم بر تغییرات مشخصه ها**

۴-۱-۵- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۱	FDP_ACC.1.1	محصول باید **خط مشیهای کنترل دسترسی** را بر روی موارد زیر اعمال کند : • **موجودیت فعال :مدیر سیستم، کاربر عادی،هیچ موجودیت فعال دیگر** • **موجودیت غیرفعال:** ○ **رکوردها، مستندات و فرا-داده** **داده متعلق به کاربران** ○ **داده احرازهویت** **داده با این معیارهاهیچ معیار داده دیگر** ○ **هیچکدام از موجودیتهای غیرفعال دیگر** • **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**
	-	۲	FDP_ACF.1.1	محصول باید **خط مشیهای کنترل دسترسی** را با توجه به موارد زیر بر روی موجودیتهای غیرفعال اعمال کند: • **هویت کاربر** • **نقشها و مجوزهای کاربر مجاز**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده میشوند** • **هیچ مشخصه ای از موجودیت فعال**
	-	۳	FDP_ACF.1.2	محصول باید قوانین زیر را اجرا کند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز کند. 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 بر اساس 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 غیرمجاز 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 کند: • **تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده** • **هیچ قانون دیگری**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۶	FDP_RIP.2.1	محصول باید تضمین کند 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.
	-	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** داده های رکورد و داده های ممیزی را بر اساس مشخصه های درهم شده **داده های کاربری ذخیره شده** پایش کند
	-	۸	FDP_SDI.2.2	هنگام تشخیص خطای صحت داده، محصول باید **در هنگام نمایش فرمهای دارای داده های حساس،اقدام به قرمز کردن ردیفهای دارای خطا** را صورت دهد.

۵-۱-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.1	- FMT_SMR.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 و هر کاربری که مجوز لازم را دارد هیچ نقش دیگری** ،محدود کند.
FMT_MSA.1	- FDP_ACC.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 **نقش‌ها و یا مجموعه دسترسی-های کاربر به قسمت های مختلف برنامه** را به **مدیر سیستم و هر کاربری که مجوز لازم را دارد** محدود نماید.
	-	۳	FMT_MSA.3.1	محصول برای مشخصه‌های امنیتی که برای اعمال **خط مشی** استفاده می‌شوند، باید مقادیر پیش فرض محدود شده‌ای 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 (۱)	- FMT_SMR.1	۵	FMT_MTD.1.1 (1)	محصول باید توانایی پرس وجو، حذف،**هیچ اقدام دیگر داده های ممیزی ،حفاظت از داده کاربری و مدیریت امنیت** را به **مدیر سیستم و هر کاربری که مجوز لازم را دارد** محدود نماید.
FMT_MTD.1 (۱)	- FMT_SMR.1	۶	FMT_MTD.1.1 (2)	محصول باید توانایی پرس‌وجو، تغییر، حذف، **هیچ کارکرددیگری تمام فرمهای سیستم حسابداری تحت مالکیت و دسترسی کاربر عادی** به **کاربر عادی** محدود نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۷	FMT_SMF.1.1	محصول باید قادر به انجام کارکردهای مدیریتی که در جدول دو آمده است باشد
FMT_SMR.1	- FIA_UID.1	۸	FMT_SMR.1.1	نقشهای زیر در محصول باید تعریف شده باشد: مدیر سیستم، کاربر عادی ، **هیچ نقش دیگر مجاز معرفی شده**
		۹	FMT_SMR.1.2	محصول، باید قادر به مرتبط نمودن کاربران با نقشها و دسترسی های مجاز تعریف شده باشند.

جدول دو - کارکردهای مدیریتی

مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دست رفتن داده ممیزی۱	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده های ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه های مورد استفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده در منابع	انتخاب هنگام اجرای حفاظت از اطلاعات باقیمانده (برای مثال، تخصیص و یا آزادسازی) که میتواند در محصول قابل پیکربندی باشد.
ورود دادههای کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت دادههای کاربری ذخیره شده۲	عملیاتی برای تشخیص یک خطای صحت داده که میتواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاشهای ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد.
مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیتها برای تنظیم کلمه عبورها

مؤلفه	عملیات مدیریتی
احراز هویت کاربر	مدیریت داده های احراز هویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احرازهویت کاربر انجام میشوند.
سازوکار احرازهویت چندگانه	مدیریت سازوکارهای احرازهویت مدیریت قوانین مرتبط با احرازهویت
شناسایی کاربر	مدیریت شناسایی کاربران مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز میتواند قبل از شناسایی کاربر انجام دهد.
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز میتواند مشخصه های امنیتی موجودیتهای فعال پیش فرض را تعریف و تغییر دهد.
مدیریت مشخصه های امنیتی	مدیریت گروهی از نقشهایی که با مشخصه های امنیتی در تعامل هستند.
مقداردهی اولیه مشخصه ها	مدیریت گروهی از نقشهایی که مقادیر اولیه را مشخص میکنند .مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول
مدیریت دادههای محصول -۱مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده های محصول
مدیریت داده های محصول -۱کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده های محصول
نقشهای امنیتی	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
محدودیت بر روی چندین نشست همزمان	مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر
برقراری نشست	مدیریت شرایط آغاز نشست توسط مدیر مجاز
خاتمه دادن به نشستها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیشفرض غیرفعال بودن کاربر که نشست خاتمه یابد.

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

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.1	- -	۱	FPT_FLS.1.1	محصول باید در زمان رخداد انواع شکستهای زیر، وضعیت امن را حفظ نمایند : **شکستهای نرم افزاری ، شکستهای سخت افزاری**
	-	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 کند
FPT_TDC.1	- -	۳	FPT_TDC.1.1	محصول در صورت استفاده از محصولات امن IT باید تفسیر سازگار **کد تاییدیه برای احراز هویت دوعامله** را در زمان اشتراک گذاری داده امنیتی بین خود و دیگر محصولات امن IT فراهم آورد
	-	۴	FPT_STM.1.1	محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و سازوکار کارکردی صحیح برطرف کند
	-	۵	FPT_TUD_EXT.1.۲	محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولیدکننده محصول فراهم کند که به روزرسانی نرم افزار و میان افزار محصول مورد ارزیابی را به صورت دستی آغاز کند و از سازوکار به روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به روزرسانی پشتیبانی کند
	-	۶	FPT_TUD_EXT.1.۳	محصول مورد ارزیابی باید در صورت استفاده از به روزرسانی به روش خودکار، پیش از نصب به روزرسانیهای نرم افزاری و میان افزاری،با استفاده از سازوکار امضای دیجیتال ابزاری را برای احراز هویت میان افزار آنها در اختیار محصول مورد ارزیابی قرار دهد.

۷-۱-۵- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.1	FPT_FLS.1 -	۱	FRU_FLT.1.1	محصول باید از عملکرد تمام کارکردهای اصلی هنگام رویداد شکستهای زیر اطمینان حاصل کند: **شکست نرم افزاری ، هیچ نوع شکست دیگری**

۸-۱-۵- 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 کند.
		۲	FTA_MCS.1.2	محصول باید به صورت پیش‌فرض، سه نشست همزمان پیش‌فرض برای هر کاربر در نظر بگیرد.
FTA_SSL.3	- -	۳	FTA_SSL.3.1	محصول باید کلیه نشستهای تعاملی راه دور را پس از مدت زمان یک عدد صحیح به دقیقه که توسط مدیر تنظیم میشود غیرفعال بودن، خاتمه دهد.
FTA_SSL.4	- -	۴	FTA_SSL.4.1	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه ی خاتمه نشست را بدهد.
FTA_TAH.1	- -	۵	FTA_TAH.1.1	در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس زمان، هیچ مشخصه دیگر باشد
FTA_TAH.1	- -	۶	FTA_TAH.1.2	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید تاریخ، زمان آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.
FTA_TAH.1	- -	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	محصول باید قادر به ممانعت از ایجاد نشست بر اساس **مکان، شماره پورت، روز، زمان، آدرس آی پی** باشد.

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

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۱	FTP_ITC.1.1	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل TLS میان خود و موجودیت IT معتبر، سرور ممیزی، سرور احرازهویت، **هیچ سرور دیگر** 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.
	-	۲	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.
	-	۳	FTP_ITC.1.3	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای **خواندن و نوشتن هرنوع اطلاعات از پایگاه داده** راه‌اندازی نماید.
	-	۴	FIA_X509_EXT.1.1/Rev	محصول مورد ارزیابی باید گواهینامه ها را بر اساس قوانین زیر تائید کند: • تائید گواهینامه RFC 5280 و تائید مسیر گواهینامه که از حداقل طول مسیر دو گواهینامه پشتیبانی میکند • مسیر گواهینامه باید با یک گواهینامه CAامن پایان یابد. • محصول مورد ارزیابی باید برای تائید یک مسیر گواهینامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچمCA برای تمام گواهینامه های CA به حالت True تنظیم شده است. • محصول مورد ارزیابی باید وضعیت فسخ گواهینامه را با استفاده از پروتکل وضعیت گواهینامه آنلاین (OCSP) مشخص شده در RFC 6960 تائید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsageرا بر اساس قوانین زیر تائید کند: ○ گواهینامه های مورداستفاده برای تائید به روزرسانیهای امن واعتبارسنجی صحت کدهای اجرایی، باید هدف Code Signing id-OID 1.3.6.1.5.5.7.3.3 با kp 3 را در فیلد extendedKeyUsage خود داشته باشند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ گواهینامه های سرور ارائهشده برای TLSباید هدف id-OID Server Authentication ۱,۳,۶,۱,۵,۵,۷,۳,۲ با kp 1 رادر فیلد extendedKeyUsage خود داشته باشند. ○ گواهینامه های کلاینت ارائه شده برای TLS باید هدف id- Server Authentication OID 1.3.6.1.5.5.7.3.2 با kp 1 رادر فیلد extendedKeyUsage خود داشته باشند. ○ گواهینامه های OCSP مورداستفاده برای پاسخهای OCSP باید هدف OCSP Signing id-OID 1.3.6.1.5.5.7.3.9 با kp 9 را در فیلد extendedKeyUsage خود داشته باشند.
	-	۵	FIA_X509_EXT.1.2/Rev	محصول مورد ارزیابی تنها درصورتیکه افزونه مربوط به basicConstraintsاز پیش تنظیم شده باشد و پرچم CAبه حالت TRUE تنظیم شده باشد، یک گواهینامه را به عنوان گواهینامه CA میپذیرد.
	-	۶	FIA_X509_EXT.2.1	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای HTTPS و **هیچ کاربرد دیگر**، هیچ کاربرد دیگر از گواهینامه های X.509v3 تعریف شده در RFC 5280استفاده کند.

۲-۵- الزامات کارکردامنیتی برنامه های کاربردی

الزامات کارکردامنیتی زیر مطابق پروفایل حفاظتی برنامه کاربردی تهیه شده‌اند.

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱	**عملیات رمزنگاری**	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲		ذخیره سازی اسرار ۱	FCS_STO_EXT.1.1
۳	**حفاظت از داده های کاربری**	دسترسی به منابع پلتفرم ۱	FDP_DEC_EXT.1.1
٤		دسترسی به منابع پلتفرم ۲	FDP_DEC_EXT.1.2
٥		ارتباطات شبکه ای ۱	FDP_NET_EXT.1.1
٦		رمزگذاری داده های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1
۷	**محرمانگی**	استفاده کاربر از یک سرویس بدون افشاء هویت ۴	FPR_ANO_EXT.1.1
۸	**مدیریت امنیت**	سازوکار پیکربندی پشتیبان شده ۱	FMT_MEC_EXT.1.1
۹		تأمین امنیت با پیکربندی پیشفرض ۱	FMT_CFG_EXT.1.1
۱۰		تأمین امنیت با پیکربندی پیشفرض ۲	FMT_CFG_EXT.1.2
۱۱		کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۱۲	**حفاظت از توابع امنیتی محصول**	استفاده از واسط برنامه نویسی کاربردی و سرویسهای پشتیبانی شده ۱	FPT_API_EXT.1.1
۱۳		قابلیتهای ضد اکسپلویت ۱	FPT_AEX_EXT.1.1
۱٤		قابلیتهای ضد اکسپلویت ۲	FPT_AEX_EXT.1.2
		قابلیتهای ضد اکسپلویت ۳	FPT_AEX_EXT.1.3

۱۵		قابلیتهای ضد اکسپلویت ۴	FPT_AEX_EXT.1.4
۱۶		قابلیتهای ضد اکسپلویت ۵	FPT_AEX_EXT.1.5
۱۷		به روزرسانی امن ۱	FPT_TUD_EXT.1.1
۱۸		به روزرسانی امن ۲	FPT_TUD_EXT.1.2
۱۹		به روزرسانی امن ۳	FPT_TUD_EXT.1.3
۲۰		به روزرسانی امن ۴	FPT_TUD_EXT.1.4
۲۱		به روزرسانی امن ۵	FPT_TUD_EXT.1.5
۲۲		به روزرسانی امن ۶	FPT_TUD_EXT.1.6
۲۳		استفاده از کتابخانه های شخص ثالث	FPT_LIB_EXT.1.1
۲۴	**کانالهای امن**	حفاظت از تبادل داده ها۱	FTP_DIT_EXT.1.1
۲۵			
۲۶	**عملیات رمزنگاری**	الزامات پروتکلTLS Client/ احراز هویت دستی ۵	FCS_TLSC_EXT.2.1
۳۷		پروتکل TLSC(۱)	FCS_TLSC_EXT.1.1
۳۸		پروتکل TLSC(۲)	FCS_TLSC_EXT.1.2
۳۹		پروتکل TLSC(۳)	FCS_TLSC_EXT.1.3
۵۳	**شناسایی و احراز هویت**	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۵۴		الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۵۵		الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۵۶		الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2

الزامات برنامه کاربردی

۱-۲-۵- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_RBG_EXT.1	-	۱	FCS_RBG_EXT.1.1	برنامه ی کاربردی برای عملیات رمزنگاری باید از هیچگونه عملکرد تولید بیت تصادفی قطعی استفاده نکند.
FCS_STO_EXT.1	-	۲	FCS_STO_EXT.1.1	برنامه‌ی کاربردی در فضای حافظه‌ی غیرفرّار باید از عملکردهای ارائه‌شده در پلت‌فرم برای ذخیره‌ی امن **گذرواژه ها و کلیدهای رمزنگاری** استفاده کند
FDP_DEC_EXT.1	-	۳	FDP_DEC_EXT.1.1	برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • اتصال شبکه
FDP_DEC_EXT.1	-	۴	FDP_DEC_EXT.1.2	برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • هیچ نوع از منابع اطلاعات حساس
FDP_NET_EXT.1	-	۵	FDP_NET_EXT.1.1	برنامه کاربردی بایدارتباطات شبکه ای خود را محدود کند به: • ارتباطاتی که کاربر برای ارتباط دوطرفه با پایگاه داده ایجاد کرده است
FDP_DAR_EXT.1	-	۶	FDP_DAR_EXT.1.1	برنامه کاربردی باید: • از عملکرد ارائه شده توسط پلتفرم برای رمزگذاری داده های حساس استفاده کند

۲-۲-۵- کلاس محرمانگی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPR_ANO_EXT.1	-	۷	FPR_ANO_EXT.1.1	برنامه کاربردی باید اطلاعات شناسایی شخصی PII را در شبکه انتقال ندهد

۳-۲-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۸	FMT_MEC_EXT.1.1	برنامه کاربردی باید سازوکار توصیه شده توسط تولیدکننده ی پلتفرم را برای ذخیره سازی و تنظیم گزینه های پیکربندی، استفاده نماید
FMT_CFG_EXT.1	-	۹	FMT_CFG_EXT.1.1	هنگامی که برنامه کاربردی بدون اعتبارنامه یا بااعتبارنامه پیشفرض پیکربندی شده است، برنامه کاربردی باید اقدامات لازم برای ایجاد اعتبارنامه جدید را فراهم آورد.
	-	۱۰	FMT_CFG_EXT.1.2	برنامه کاربردی باید به طور پیش فرض طوری پیکربندی شود که با قرار دادن مجوزهای دسترسی به فایل مناسب، خود برنامه کاربردی و داده های آن را از دسترسیهای غیرمجاز محافظت کند.
	-	۱۱	FMT_SMF.1.1	محصول باید قابلیت اجرای کارکردهای امنیتی زیر را داشته باشد: بدون کارکرد مدیریتی **هیچ کارکرد مدیریتی دیگر**

۴-۲-۵- کلاس حفاظت از محصول

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_API_EXT.1	-	۱۲	FPT_API_EXT.1.1	برنامه کاربردی باید تنها از واسط برنامه نویسی کاربردیهای (API) پلتفرم پشتیبانی شده استفاده کند
FPT_AEX_EXT.1	-	۱۳	FPT_AEX_EXT.1.1	برنامه کاربردی جز برای **هیچ استثنا صریح و واضحی**، نباید درخواست نگاشت حافظه به آدرس مشخصی نماید.
	-	۱۴	FPT_AEX_EXT.1.2	برنامه کاربردی باید: هیچ بخشی از حافظه را همزمان هم به نوشتن اطلاعات و هم اجرای مجوزها اختصاص ندهد
	-	۱۵	FPT_AEX_EXT.1.3	برنامه کاربردی باید با امکانات امنیتی که توسط تولیدکننده ی پلتفرم ارائه شده است، سازگار باشد
	-	۱۶	FPT_AEX_EXT.1.4	برنامه کاربردی نباید فایلهایی را که توسط کاربر قابل تغییر هستند در دایرکتوریهایی بنویسد که حاوی فایلهای اجرایی اند، مگر اینکه کاربر به طور مستقیم چنین دایرکتوری ها را انتخاب نماید.
	-	۱۷	FPT_AEX_EXT.1.5	برنامه کاربردی باید با قابلیت محافظت از سرریز بافر مبتنی بر پشته کامپایل شود
FPT_TUD_EXT.1	-	۱۸	FPT_TUD_EXT.1.1	برنامه کاربردی باید این قابلیت را ارائه کند که به روزرسانی ها و وصله های برنامه های کاربردی را بررسی نماید
	-	۱۹	FPT_TUD_EXT.1.2	برنامه کاربردی باید با استفاده از قالب مدیریت بسته که توسط آن پلتفرم پشتیبانی میشود، توزیع و منتشر شود
	-	۲۰	FPT_TUD_EXT.1.3	برنامه کاربردی باید طوری بسته بندی شود که حذف آن، منجر به پاک شدن تمامی آثار برنامه کاربردی شود؛ به استثناء تنظیمات پیکربندی، فایلهای خروجی و ثبت وقایع/ ممیزی
	-	۲۱	FPT_TUD_EXT.1.4	برنامه کاربردی نباید کد باینری خود را دانلود، اصلاح، جایگزین یا به روزرسانی کند

	-	۲۲	FPT_TUD_EXT.1.5	برنامه کاربردی باید این قابلیت را ارائه کند تا نسخه فعلی برنامه کاربردی را بازیابی کند
	-	۲۳	FPT_TUD_EXT.1.6	بسته ی نصب برنامه کاربردی و نسخه های به روزرسانی آن باید به طور دیجیتالی امضا شوند به طوریکه پلتفرم بتواند رمزنگاری آنان را قبل از نصب برنامه کاربردی، چک کند
FPT_LIB_EXT.1	-	۲۴	FPT_LIB_EXT.1.1	هدف از این الزام آن است که ارزیاب کتابخانه های شخص ثالث غیرضروری یا پیش بینی نشده در برنامه کاربردی را تشخیص و ثبت نماید. این شامل کتابخانه هایی که جهت امور تبلیغاتی ایجادشده اند نیز میشود که میتواند تهدیدی برای حریم خصوصی به شمار رود. همچنین شامل تضمین مستندسازی این کتابخانه ها برای مواقعی که آسیب پذیری هایی در آینده کشف شوند نیز است.

۵-۲-۵- کلاس کانالها و مسیرهای امن

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_DIT_EXT.1	-	۲۵	FTP_DIT_EXT.1.1	برنامه کاربردی باید بین خود و دیگر محصولات مورد اعتماد IT تمامی داده های حساس مورد تبادل را با استفاده از حداقل یکی از این TLS رمزگذاری کند
	-	۲۷	FCS_TLSC_EXT.2.1	برنامه کاربردی باید با استفاده از گواهی X.509v3 از احراز هویت متقابل (دوسویه) پشتیبانی نماید.
	-	۳۷	FCS_TLSC_EXT.1.1	برنامه کاربردی باید با پشتیبانی از مجموعه رمز الیست شده در زیر، TLS 1.2 ارائه شده توسط پلتفرم را درخواست نماید، TLS 1.2(RFC 5246) پیاده‌سازی نماید مجموعه رمز الزامی: TLS_DHE_RSA_WITH_AES_128_CBC_SHA به صورت تعریف شده در RFC 5246
	-	۳۸	FCS_TLSC_EXT.1.2	برنامه کاربردی باید منطبق بودن شناسه ارائه شده با شناسه مرجع را بر طبق RFC 6125 وارسی نماید.
	-	۳۹	FCS_TLSC_EXT.1.3	برنامه کاربردی باید در صورت معتبر بودن گواهی همتا، تنها یک کانال امن برقرار نماید.

	-	۵۳	FIA_X509_EXT.1.1

برنامه کاربردی باید کارکرد ارائه شده توسط پلتفرم را درخواست نماید تا مطابق با قوانین زیر، گواهی‌ها را معتبر نماید:

- اعتبارسنجی گواهی و مسیر گواهی RFC 5280
- مسیر گواهی باید با یک گواهی CA امن خاتمه یابد.
- برنامه کاربردی باید مسیر گواهی را اعتبارسنجی نماید با تضمین نمودن وجود آیتم basicConstraints و اینکه پرچم CA برای تمامی گواهینامه‌ها وضعیت TRUE داشته باشد.
- برنامه کاربردی باید وضعیت لغو گواهی را با استفاده از پروتکل وضعیت گواهی آنلاین (OCSP) به صورت مشخص شده در RFC 2560
- برنامه کاربردی باید فیلد extendedKeyUsage را مطابق با قوانین زیر اعتبارسنجی نماید:
  - گواهی استفاده شده برای بروزرسانی امن و بررسی صحت کد اجرایی باید در فیلد extendedKeyUsage دارای هدف Code Signing باشد (id-kp 3 با OID 1.3.6.1.5.5.7.3.3)
  - گواهی‌های سرور ارائه شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احرازهویت سرور باشد (id-kp 1 با OID 1.3.6.1.5.5.7.3.1)
  - گواهی‌های کلاینت ارائه شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احرازهویت کلاینت باشد (id-kp 2 با OID 1.3.6.1.5.5.7.3.2)
  - گواهی‌های S/MIME ارائه شده برای امضاء و رمزنگاری ایمیل باید در فیلد extendedKeyUsage دارای هدف حفاظت از ایمیل باشد (id-kp 4 با OID 1.3.6.1.5.5.7.3.4)
  - گواهی‌های OCSP ارائه شده برای پاسخ‌های OCSP باید در فیلد extendedKeyUsage دارای هدف امضای OCSP باشد (id-kp 9 با OID 1.3.6.1.5.5.7.3.9)
  - گواهی‌های سرور ارائه شده برای EST باید در فیلد extendedKeyUsage دارای هدف مرکز ثبت گواهی CMC باشد (id-kp-cmcRA با OID 1.3.6.1.5.5.7.3.28)

	-	۵۴	FIA_X509_EXT.1.2	برنامه کاربردی باید در صورت وجود basicConstraints extension و true بودن CA Flag، گواهی را به عنوان گواهی CA تلقی نماید.
	-	۵۵	FIA_X509_EXT.2.1	برنامه کاربردی باید از گواهی X.509v3 به صورت تعریف شده توسط RFC 5280 استفاده نماید تا از احرازهویت برای HTTPS پشتیبانی نماید.
	-	۵۶	FIA_X509_EXT.2.2	زمانیکه برنامه کاربردی نمی‌تواند جهت تعیین اعتبار گواهی، اتصالی را برقرار نماید؛ برنامه کاربردی باید گواهی پذیرفته نمی‌شود.

۳-۵- الزامات تضمین امنیتی

الزامات عملکرد تضمین تو صیف کننده چگونگی ارزیابی هدف ارزیابی ا ست. در این بخش الزامات EAL1 آورده می شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام مؤلفه	توضیحات
Development	**ADV_FSP.1**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.1**	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	**ATE_IND.1**	آزمون مستقل-منطبق
Vulnerability Assessment	**AVA_VAN.1**	تحلیل آسیب پذیری
Life cycle Support	**ALC_CMC.1**	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی
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

بخش توجیهات

الزامات زیر مربوط به پروفایل حفاظتی برنامه کاربردی تحت شبکه در محصول پیاده سازی نمیشوند:

شماره الزام	شرح	المان	توضیحات
۲۱	ورود داده کاربری به محصول با مشخصه امنیتی۱	FDP_ITC.2.1	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
۲۲	ورود داده کاربری به محصول با مشخصه امنیتی۲	FDP_ITC.2.2	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
۲۳	ورود داده کاربری به محصول با مشخصه امنیتی۳	FDP_ITC.2.3	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
-	ورود داده کاربری به محصول با مشخصه امنیتی ۴	FDP_ITC.2.4	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
-	ورود داده کاربری به محصول با مشخصه امنیتی ۵	FDP_ITC.2.5	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
۲۴	خروج داده کاربری از محصول با مشخصه امنیتی۱	FDP_ETC.2.1	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
۲۵	خروج داده کاربری از محصول با مشخصه امنیتی۲	FDP_ETC.2.2	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
-	خروج داده کاربری از محصول با مشخصه امنیتی ۳	FDP_ETC.2.3	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
۲۶	خروج داده کاربری از محصول با مشخصه امنیتی۴	FDP_ETC.2.4	ورود و خروج داده کاربری با مشخصه امنیتی نداریم
-	سازگاری داده امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.1.2	داده‌های دریافتی از دیگر محصولات نداریم
۶۰	مسیر امن ۱	FTP_TRP.1.1	هیچگونه فعالیت از راه دور در محصول نداریم
۶۱	مسیر امن ۲	FTP_TRP.1.2	هیچگونه فعالیت از راه دور در محصول نداریم
۶۲	مسیر امن ۳	FTP_TRP.1.3	هیچگونه فعالیت از راه دور در محصول نداریم
۶۳	تولید کلید رمزنگاری ۱	FCS_CKM.1.1	عدم وجود کلیدهای رمزنگاری نامتقارن در سیستم

۶۶	عملیات رمزنگاری ۱(۴)	FCS_COP.1.1(4)	عدم وجود امضاء دیجیتال و عدم وجود کلید رمزنگاری نامتقارن در محصول
۷۳	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4	عدم وجود مجموعه رمز منحنی بیضوی در محصول

الزامات زیر مربوط به پروفایل حفاظتی برنامه کاربردی در محصول پیاده سازی نمیشوند:

شماره الزام	شرح	المان	توضیحات
۱۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1	بعلت ماهیت شبکه ای بودن محصول
۱۹	به روزرسانی امن ۲	FPT_TUD_EXT.1.2	ماهیت محصول بصورت dll های مجزا هست
۲۷	الزامات پروتکلTLS Client/ احراز هویت دستی ۵	FCS_TLSC_EXT.2.1	نحوه احراز هویت دوگانه بوسیله توکن نیست
۲۸	تولید بیت تصادفی ۳	FCS_RBG_EXT.2.1	
۲۹	تولید بیت تصادفی ۴	FCS_RBG_EXT.2.2	
۳۰	مدیریت کلید رمزنگاری ۵	FCS_CKM_EXT.1.1	
۳۱	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1(1)	
۳۲	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1	
۳۳	عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)	FCS_COP.1.1(1)	
۳۴	عملیات رمزنگاری – درهم سازی ۱ (۲)	FCS_COP.1.1(2)	
۳۵	عملیات رمزنگاری – امضاء ۱ (۳)	FCS_COP.1.1(3)	
۳۶	عملیات رمزنگاری – امضاء ۲ (۴)	FCS_COP.1.1(4)	
۴۰	پروتکل TLSC (۷)	FCS_TLSC_EXT.4.1	عدم وجود مجموعه رمز منحنی بیضوی در محصول