به نام خدا

سند هدف امنیتی نظام جامع پذیرش و بررسی پیشنهادها-۸.۸.۲

شرکت نرم افزاری جادوی فکر

اردیبهشت ماه ۱۴۰۲

نسخه ۲.۲

فهرست

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سند هدف امنیتی نظام جامع پذیرش و بررسی پیشنهادها-۸.۸.۲
نسخه	۲.۲
تاریخ	اردیبهشت ۱۴۰۲
نویسندگان	سیدمحمدسعید منافی، حسین اندرخورا

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت نرم افزاری جادوی فکر
نام محصول	نظام جامع پذیرش و بررسی پیشنهادها
نوع محصول	برنامه کاربردی تحت شبکه
نسخه	۸.۸.۲

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

توابع امنیتی اصلی سامانه به صورت کلی شامل موارد زیر است:

- احراز هویت
- مدیریت امنیت
- کنترل دسترسی
- رویداد نگاری
- مدیریت ارتباط با کاربر
- مدیریت ارتباط با وب سرویس پیامک

۱-۳-۲- نوع هدف ارزیابی

هدف ارزیابی برنامه کاربردی تحت وب است

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

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

کامپوننت‌ها	حداقل الزامات
حافظه (RAM)	حداقل ۴ گیگا بایت
فضای آزاد بر روی دیسک	حداقل ۵۰۰ مگابایت برای نصب اولیه
پایگاه داده	SQL Server 2014 یا نسخه جدیدتر
مرورگر وب	Firefox 33 یا نسخه جدیدتر، Chrome 35 یا نسخه جدیدتر
سایر نرم افزار ها	.Net Framework 4.5

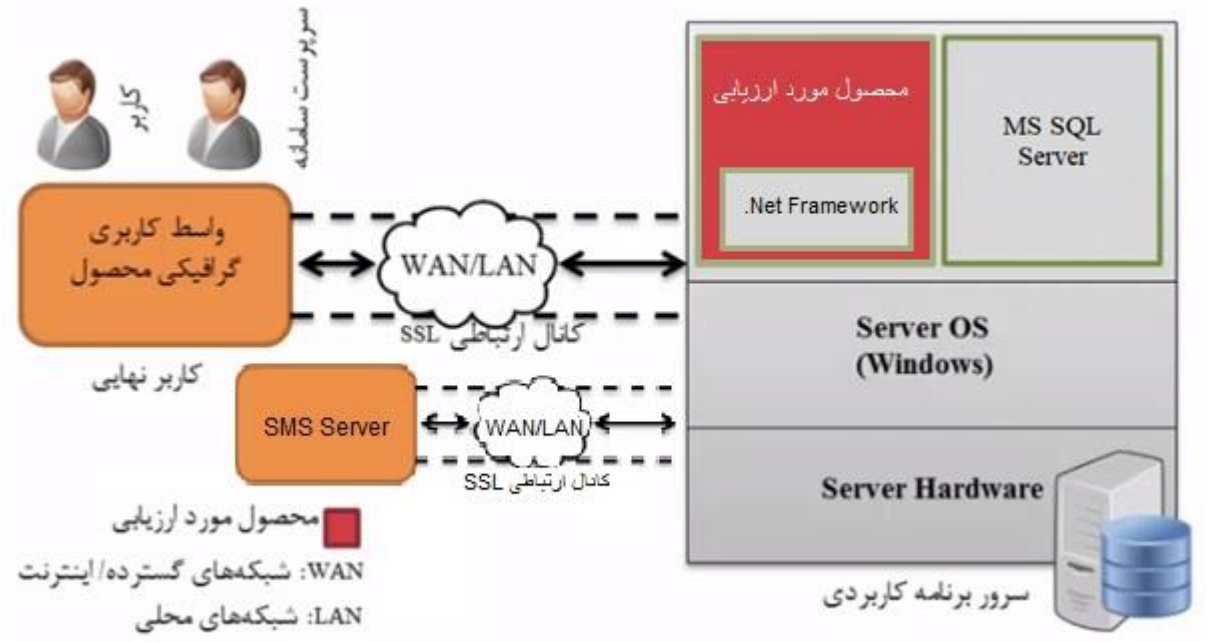
۴-۱- توصیف هدف ارزیابی

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
سامانه نظام پیشنهادها	نسخه ۸.۸.۲
پایگاه داده	Sql Server 2014 یا نسخه بالاتر
IIS (Internet Information Services)	نسخه 8 یا نسخه بالاتر

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



۲-۴-۱- حوزه منطقی

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

کارکردها	توصیف
احراز هویت	احراز هویت کاربر با استفاده از نام کاربری و کلمه عبور. استفاده از پیامک برای احراز هویت دومرحله ای.
مدیریت امنیت	امکان اعمال تنظیمات توسط مدیر سامانه برای کنترل امنیت سامانه در بخش های مختلف. کنترل صحت داده های حساس ذخیره شده در پایگاه داده.
کنترل دسترسی	سامانه دارای امکان دسترسی محدود میباشد، به طوریکه هر موجودیت تنها به منوها و صفحات مربوط به خود دسترسی دارد. برای کاربران مجاز کنترل دسترسی معمولا با استفاده از داده احراز هویت انجام می شود.
رویداد نگاری	ثبت ورود و خروج کاربران و فعالیت هایی که در سامانه انجام می دهند.
مدیریت ارتباط با کاربر	مدیریت ارتباط محصول با کاربران تا ارتباطی امن برقرار شود و امکان سرقت هویت کاربران وجود نداشته باشد.
مدیریت ارتباط با وب سرویس پیامک	مدیریت ارتباط محصول با وب سرویس پیامک تا ارتباط از طریق بستری امن بین محصول سرویس دهنده برقرار شود.

۲- ادعای انطباق

۲-۱- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
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	پروفایل حفاظتی برنامه های کاربردی تحت شبکه، مرکز مدیریت راهبردی افتا، اسفند ماه ۹۶ – نسخه ۱.۱

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	EAL1

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.
ارتباطات امن مبتنی بر TLS	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.
پیکربندی مناسب	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 خط-مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	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 نماید. 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 تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم می‌تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند.

تهدید	توصیف
	مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و داده‌های حفاظت شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نمی‌باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. و بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می‌باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشای اطلاعات	داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می‌تواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص می‌باشد که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDoS می‌باشد که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده‌های ورودی مخرب	مهاجم می‌تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم می‌تواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر رابه دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.

۳-۳- فرضیات

فرضیه	توصیف
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
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 آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
محیط امن	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت می‌گیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره‌سازی و دیگر مولفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داده‌ای از دست نمی‌رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی‌دهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.
تحویل امن	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.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی برای محصول

هدف امنیتی	توصیف
ممیزی	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.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احرازهویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف شده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
صحت داده	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.

هدف امنیتی	توصیف
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقشهای کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید.
مدیریت خطا	محصول باید صورت امن و کارامد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت دادههای باقیمانده	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 می-گردد.

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 مؤلفهها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفههای 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 می-توان به غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانههای 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 مینمایند.

هدف امنیتی	توصیف
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده‌ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری-های امنیتی شناخته شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه‌های 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.
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 غیر قابل دسترس گردند.
پشتیبان‌گیری مناسب	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 مؤلفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

۵- نیازمندی‌های امنیتی

۵-۱- الزامات کارکرد امنیتی

الزامات ذکر شده در این بخش برگرفته از پروفایل حفاظتی سامانه های کلاینت/سرور است. نوتاسیون مورد استفاده در این بخش به این صورت است که عملیات انتخاب به صورت underlined و عملیات اختصاص با استایل bold نمایش داده خواهند شد.

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.1.2
۶		**بازبینی داده ممیزی محدود ۱**	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	پشتیبانی از رمزنگاری	**عملیات رمزنگاری ۱ (۱)**	FCS_COP.1.1(1)
۱۴		**عملیات رمزنگاری ۱ (۲)**	FCS_COP.1.1(2)
۱۵	حفاظت از داده‌های کاربری	**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**	FDP_RIP.2.1

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
		منابع ۱	
۲۱		ورود داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.2.1
۲۲		ورود داده کاربری به محصول با مشخصه امنیتی۲	FDP_ITC.2.2
۲۳		ورود داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.2.3
۲۴		ورود داده کاربری به محصول با مشخصه امنیتی ۴	FDP_ITC.2.4
۲۵		ورود داده کاربری به محصول با مشخصه امنیتی ۵	FDP_ITC.2.5
۲۶		خروج داده کاربری از محصول با مشخصه امنیتی ۱	FDP_ETC.2.1
۲۷		خروج داده کاربری از محصول با مشخصه امنیتی ۲	FDP_ETC.2.2
۲۸		خروج داده کاربری از محصول با مشخصه امنیتی ۳	FDP_ETC.2.3
۲۹		خروج داده کاربری از محصول با مشخصه امنیتی ۴	FDP_ETC.2.4
۳۰		صحت داده های کاربری ذخیره شده ۲	FDP_SDI.2.1
۳۱		صحت داده های کاربری ذخیره شده ۳	FDP_SDI.2.2
۳۲	شناسایی و احراز هویت	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۳۳		مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۳۴		تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۳۵		مدیریت کلمه عبور	FIA_PMG_EXT.1.1
۳۶		شناسایی قبل از هر اقدام ۱	FIA_UID.1.1
۳۷		شناسایی قبل از هر اقدام ۲	FIA_UID.1.2
۳۸		سازوکار احرازهویت چندگانه ۱	FIA_UAU.5.1
۳۹		سازوکار احرازهویت چندگانه ۲	FIA_UAU.5.2

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۴۰		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۴۱		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۴۲		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۴۳	مدیریت امنیت	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۴۴		مدیریت مشخصه‌های امنیتی 1	FMT_MSA.1.1
۴۵		مدیریت مشخصه های امنیتی ۳	FMT_MSA.3.1
۴۶		مدیریت مشخصه های امنیتی ۴	FMT_MSA.3.2
۴۷		مدیریت داده های محصول ۱ – مدیر سیستم	FMT_MTD.1.1 (1)
۴۸		مدیریت داده های محصول ۱ – کاربر عادی، وارد کننده	FMT_MTD.1.1 (2)
۴۹		کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۵۰		نقش‌های امنیتی ۱	FMT_SMR.1.1
۵۱		نقش‌های امنیتی ۲	FMT_SMR.1.2
۵۲	حفاظت از توابع امنیتی محصول	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۵۳		انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۵۴		سازگاری داده های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۵۵		سازگاری داده های امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.1.2
۵۶		به روز رسانی امن ۲	FPT_TUD_EXT.1.2
۵۷	کلاس تخصیص منابع	تحمل خطا ۱	FRU_FLT.1.1
۵۸	دسترسی به محصول	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۹		محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۶۰		محدودیت بر روی چندین نشست همزمان ۱	FTA_SSL.3.1
۶۱		خاتمه دادن به نشست ها توسط کاربر ۱	FTA_SSL.4.1
۶۲		سوابق دسترسی به محصول ۱	FTA_TAH.1.1
۶۳		سوابق دسترسی به محصول ۲	FTA_TAH.1.2
۶۴		سوابق دسترسی به محصول ۳	FTA_TAH.1.3
۶۵		برقراری نشست ۱	FTA_TSE.1.1
۶۶	کانال‌ها و مسیرهای مورد اعتماد	مسیر امن ۱	FTP_TRP.1.1
۶۷		مسیر امن ۲	FTP_TRP.1.2
۶۸		مسیر امن ۳	FTP_TRP.1.3
۶۹		کانال امن ۱	FTP_ITC.1.1
۷۰		کانال امن ۲	FTP_ITC.1.2
۷۱		کانال امن ۳	FTP_ITC.1.3
	الزامات پیوست دو		
۷۲	الزامات پروتکل HTTPS	الزامات پروتکل HTTPS (۱)	FCS_HTTPS_EXT.1.1
۷۳		الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۷۴		الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۷۵	الزامات پروتکل TLS Client/ احراز هویت	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۷۶		الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۷۷		الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۷۸		الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۷۹	الزامات پروتکل TLS Server/ احراز هویت	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۸۰		الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۸۱		الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۸۲	الزامات شناسایی و احراز هویت	الزامات پروتکل X509 (۱) / ابطال	FIA_X509_EXT.1.1/Rev
۸۳		الزامات پروتکل X509 (۲) / ابطال	FIA_X509_EXT.1.2/Rev
۸۴		الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۸۵		الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2

۱-۱-۵- کلاس ممیزی امنیت

<table>
<tr><th>مؤلفه</th><th>وابستگی ها</th><th>شماره</th><th>المان</th><th>شرح المان</th></tr>
<tr><td>FAU_GEN.1</td><td>FPT_STM.1 -</td><td>۱</td><td>FAU_GEN.1.1</td><td>محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:
• آغاز و اتمام توابع ممیزی؛
• رویدادهای قابل ممیزی (این رویدادها در جدول زیر آمده است)،
<table>
<tr><th>مولفه</th><th>رویداد قابل ممیزی</th><th>جزئیات</th></tr>
<tr><td>FAU_SAR.1</td><td>(Minimal)خواندن اطلاعات از رکوردهای ممیزی</td><td></td></tr>
<tr><td>FAU_SAR.2</td><td>(Minimal) تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی</td><td></td></tr>
<tr><td>FAU_SEL.1</td><td>(Minimal) تغییرات انجام شده بر روی تنظیمات ممیزی در حالیکه تابع ممیزی فعال است.</td><td></td></tr>
<tr><td>FAU_STG.3</td><td>(Minimal) عملیاتی که در هنگام عبور از حد آستانه تابع ممیزی روی میدهد.</td><td></td></tr>
<tr><td>FAU_STG.4</td><td>(Minimal) عملیات انجام شده به دلیل شکست ذخیره سازی ممیزی</td><td></td></tr>
<tr><td>FCS_COP.1(1)</td><td>• (Minimal)موفقیت یا شکست، و نوع عملیات رمزنگاری
• (basic)هر مد عملیاتی قابل اعمال رمزنگاری، ویژگی های موجودیت فعال و غیرفعال</td><td></td></tr>
<tr><td>FCS_COP.1(2)</td><td>• (Minimal)موفقیت یا شکست، و نوع عملیات رمزنگاری</td><td></td></tr>
</table>
</td></tr>
</table>

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
					• (basic)هر مد عملیاتی قابل اعمال رمزنگاری، ویژگی های موجودیت فعال و غیرفعال	
				FDP_ACF.1	• (Minimal)درخواست های موفق برای اجرای عملیات بر روی یک موجودیت غیرفعال تحت پوشش سیاست توابع امنیتی • (basic)تمامی درخواست‌های موفق و ناموفق برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	شناسایی داده های موجودیت غیرفعال
				FDP_ITC.2	• (Minimal) ورود موفق داده کاربری، شامل هر مشخصه های امنیتی • (basic) همه تلاش ها برای ورود داده کاربر، شامل هر مشخصه های امنیتی	
				FDP_ETC.2	• (Minimal) خروج موفق اطلاعات • (basic) همه تلاش ها برای خروج اطلاعات	
				FDP_SDI.2	• (Minimal) تلاش های موفق برای بررسی صحت داده کاربر، شامل یک نشانه از نتایج بررسی • (basic) همه تلاش ها برای بررسی صحت داده کاربر، شامل یک نشانه از نتایج بررسی اگر انجام	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
					شده باشد.	
				FIA_AFL.1	(Minimal) رسیدن به حد آستانه برای تلاش های احرازهویت ناموفق و اقداماتی (برای مثال غیرفعال کردن ترمینال) که انجام مشود و عواقب اگر مناسب بود، برگرداندن سامانه به وضعیت عادی (برای مثال فعال سازی مجدد یک ترمینال)	
				FIA_UAU.1	•(Minimal) استفاده ناموفق از مکانیزم احرازهویت •(basic) همه استفاده ها از مکانیزم احرازهویت	
				FIA_UAU.5	•(Minimal) آخرین تصمیم برای احرازهویت •(basic) نتیجه هر مکانیزم فعال شده همراه با تصمیم نهایی	
				FIA_UID.1	•(Minimal) استفاده ناموفق از مکانیزم شناسایی کاربر، از جمله هویت کاربران ارائه شده. •(basic) همه استفاده ها از مکانیزم شناسایی کاربر(موفق و ناموفق)، از جمله هویت کاربران ارائه شده.	
				FIA_USB.1	•(Minimal) پیوند ناموفق ویژگی های امنیتی کاربر با موجودیت فعال (برای مثال ایجاد یک کاربر) •(basic) پیوند موفق و ناموفق ویژگی های امنیتی کاربر با موجودیت فعال (برای مثال ایجاد موفق یا ناموفق یک کاربر)	
				FMT_MOF.1	(basic) تمامی تغییرات بر روی رفتار توابع امنیتی هدف ارزیابی	
				FMT_MSA.1	(basic) تمامی تغییرات بر روی مقادیر مشخصه‌های	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
					امنیتی	
				FMT_MSA.3	(basic) تغییرات بر روی تنظیمات پیشفرض قوانین محدودکننده و یا مجاز (basic) تمامی تغییرات بر روی مقادیر اولیه مشخصه-های امنیتی	
				FMT_MTD.1 (1)	(basic) تمامی تغییرات بر روی مقادیر دادههای توابع امنیتی	
				FMT_MTD.1 (2)	(basic) تمامی تغییرات بر روی مقادیر دادههای توابع امنیتی	
				FMT_SMF.1	(minimal) استفاده از توابع مدیریتی	
				FMT_SMR.1	(minimal) تغییرات بر روی گروهی از کاربران بخشی از یک نقش است	
				FPT_FLS.1	(basic) شکست توابع امنیتی	
				FPT_TDC.1	(minimal) موفقیت استفاده از مکانیزم سازگار داده توابع امنیتی. (basic) استفاده از مکانیزم های سازگار داده توابع امنیتی	
				FRU_FLT.1	(minimal) هر شکستی که توسط توابع امنیتی شناسایی میشود (basic) همه قابلیت های محصول که به علت شکست متوقف میشود.	
				FTA_MCS.1	(minimal) عدم پذیرش یک نشست جدید بر اساس محدودیت چندین نشت های همزمان	
				FTA_SSL.3	(minimal) پایان دادن به یک نشست توسط مکانیزم	

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				قفل نشست FTA_SSL.4 (minimal) پایان دادن به یک نشست توسط کاربر مدیریت کلمه عبور: تلاش موفق و ناموفق ورود کاربر (برای مثال، رد و یا قبول کلمه عبور کاربر)
		۲	**FAU_GEN.1.2**	محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد **[شناسه کاربری و توضیحات فعالیت.]**
FAU_GEN.2	- FAU_GEN.1 - FIA_UID.1	۳	**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 نماید.
FAU_SAR.1	- FAU_GEN.1	۴	**FAU_SAR.1.1**	محصول باید امکان خواندن/مشاهده **همه رویدادهای انتخاب شده جهت ممیزی** از کل رکوردهای ممیزی را برای **ممیز سامانه** فراهم نماید.
		۵	**FAU_SAR.1.2**	محصول باید رکوردهای ممیزی را طوری فراهم نماید که کاربر بتواند آن‌ها را درک و اطلاعات این رکوردها را تفسیر نماید.
FAU_SAR.2	- FAU_SAR.1	۶	**FAU_SAR.2.1**	محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_SAR.3		۷	**FAU_SAR.3.1**	محصول باید امکان انجام **مرتب سازی** رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس **نام کاربری، تاریخ/زمان، توضیحات و نوع عملیات** مرتب نماید.
FAU_SEL.1	- FAU_GEN.1 - FMT_MTD.1	۸	**FAU_SEL.1.1**	محصول باید قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه‌های زیر باشد: • نوع رخداد
FAU_STG.1	- FAU_GEN.1	۹	**FAU_STG.1.1**	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت نماید.
		۱۰	**FAU_STG.1.2**	محصول باید قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در محل ذخیره سازی آنها باشد.
FAU_STG.3	- FAU_STG.1	۱۱	**FAU_STG.3.1**	محصول در صورت تجاوز دنباله ممیزی از **محدودیت از پیش تعریف شده** باید با استفاده از **پیام کوتاه مدیر سامانه** را مطلع نماید.
FAU_STG.4		۱۲	**FAU_STG.4.1**	محصول در صورت پر شدن دنباله ممیزی، باید روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید و **یک هشدار برای مدیر سامانه ارسال نمایند**.

۲-۱-۵- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.1	-	۱۳	FCS_COP.1.1(1)	محصول باید [**برای وارسی صحت داده های ممیزی و داده های رکـورد**] بـر اسـاس یک الگوریتم رمزنگاری مشخص [**SHA256**] و اندازه کلیک رمز نگاری [**هیچ کدام**] اجـرا شود که مطابق با [**FIPS Pub 180-4**] باشد.
		۱۴	FCS_COP.1.1(2)	محصول باید [**تولید داده درهم‌سازی**] بـر اسـاس یـک الگـوریتم رمزنگـاری مشـخص [**HMAC-SHA256**] و اندازه کلیک رمز نگاری [**هیچ کدام**] کـه مطـابق بـا [**FIPS Pub 180-4**] باشد.

۳-۱-۵- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1	FDP_ACF.1 -	۱۵	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید: • **[موجودیت فعال: [مدیر سیستم، کاربر عادی، [هیچ موجودیت فعال دیگری]]** • **موجودیت غیرفعال:** ○ **رکوردها، مستندات** ○ **داده‌های متعلق به کاربر** ○ **داده احرازهویت** ○ **داده با این معیارها: [سطح دسترسی کاربران به صفحات و اطلاعات پرداخت های ثبت شده]** ○ **[هیچ مورد دیگری]** • **عملیات:** ○ **ایجاد موجودیت غیرفعال جدید** ○ **حذف موجودیت غیرفعال** ○ **تغییر دسترسی‌ها به موجودیت غیرفعال** ○ **عملیات بر روی فرداده‌های وابسته به موجودیت غیرفعال** ○ **[هیچ مورد دیگری]]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACF.1	- FDP_ACC.1 - FMT_MSA.3	۱۶	**FDP_ACF.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: • **[هویت کاربر** • **نقش‌ها و مجوزهای کاربر مجاز** • **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند** • **[هیچ مشخصه موجودیت فعال دیگری]]**
		۱۷	**FDP_ACF.1.2**	محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نمایند: **[عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.]**
		۱۸	**FDP_ACF.1.3**	محصول باید براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • **[کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه شده توسط محصول دسترسی دارند.** • **کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.** • **[هیچ قانون دیگری]]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۱۹	**FDP_ACF.1.4**	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: • **[تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[1] از پیش تعریف شده،** • **[هیچ قانون دیگر]]**
FDP_RIP.2	-	۲۰	**FDP_RIP.2.1**	محصول باید تضمین نماید در هنگام **[آزادسازی منابع]** تمام موجودیت‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.
FDP_ITC.2	-	۲۱	**FDP_ITC.2.1**	محصول باید هنگام دریافت داده کاربری، **[کنترل دسترسی کاربر به صفحات]** را اعمال نماید.
		۲۲	**FDP_ITC.2.2**	محصول باید از مشخصه‌های امنیتی مرتبط با داده کاربری هنگام وارد کردن داده استفاده نماید. مشخصات امنیتی شامل مواردی از این قبیل است: نوع داده، حجم و اندازه فایل، فرمت فایل، تعداد دفعات Import و از این قبیل موارد.
		۲۳	**FDP_ITC.2.3**	محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه‌های امنیتی و داده کاربری دریافت شده، فراهم می-نماید.

[1] Threshold

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۲۴	**FDP_ITC.2.4**	محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، می‌باشد.
		۲۵	**FDP_ITC.2.5**	محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی زیر را اعمال نماید: • هیچ قانون اضافه ای علاوه بر مکانیزم کنترل دسترسی بر اساس نقش در نظر گرفته نمی شود
FDP_ETC.2	-	۲۶	**FDP_ETC.2.1**	محصول باید هنگام خروج داده کاربری به بیرون[۲] [**خط‌مشی کنترل دسترسی**] را اعمال نماید
		۲۷	**FDP_ETC.2.2**	محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون از محصول)، مشخصه-های امنیتی مرتبط با داده کاربری را نیز انتقال دهد.
		۲۸	**FDP_ETC.2.3**	محصول باید اطمینان دهد که مشخصه‌های امنیتی در هنگام خروج داده از محصول، ارتباط و پیوند شفافی با داده کاربری خارج شده دارند.
		۲۹	**FDP_ETC.2.4**	محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال نماید: [**مدیر سیستم باید خروج رکوردها را محدود نماید، به طوری‌که کاربران محصول، قادر به خروج بدون هدف داده به بیرون از آن (خارج از محصول) نباشند.**]
FDP_SDI.2	FDP_SDI.1 -	۳۰	**FDP_SDI.2.1**	محصول باید داده کاربری ذخیره شده در مکان تحت کنترل خود را برای [**خطاهای**]

[2] Export user data

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				صحت داده] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های [**درهم شده**[۳] **داده‌های کاربری ذخیره شده]** پایش نماید.
		۳۱	**FDP_SDI.2.2**	هنگام تشخیص خطای صحت داده، محصول باید [**اطلاعات دارای نقص را در صـفحه میزکار مدیر سامانه]** نمایش دهد.

[3] Hash

۴-۱-۵- کلاس شناسایی و احراز هویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_AFL.1	FIA_UAU.1 -	۳۲	**FIA_AFL.1.1**	محصول، باید بتواند با استفاده از [**یک عدد مثبت قابل تنظیم توسط مدیر**] تلاش ناموفق احراز هویت مرتبط با [**تلاش کاربر برای احرازهویت شدن**] را تشخیص دهد.
		۳۳	**FIA_AFL.1.2**	زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [**به حد تعیین شده رسید و یا از آن بیشتر شد**]، محصول باید [**قفل نمودن کاربر مورد نظر**] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.
FIA_ATD.1	-	۳۴	**FIA_ATD.1.1**	محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: • **[شناسه کاربر** • **متد احرازهویت مورد استفاده** • **داده های احراز هویت** • **نقش کاربر** • **وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)** • **[آخرین زمان ورود موفق** • **تعداد تلاش نا موفق** • **آخرین زمان تغییر کلمه عبور** • **آخرین زمان قفل شدن حساب کاربری]]**
FIA_PMG_EXT.1	-	۳۵	**FIA_PMG_EXT.1.1**	محصول باید قابلیت‌های مدیریت رمزعبور را که در زیر ذکر شده‌اند برای رمزهای عبور مدیریتی فراهم نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص: ["@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(", ")"، [**کاراکتر فاصله**]] باشند. حداقل طول رمزعبور باید توسط مدیر امنیت، قابل تنظیم بوده و از رمزعبور ۸ کاراکتر یا بیشتر پشتیبانی نماید.
FIA_UID.1	-	۳۶	**FIA_UID.1.1**	محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: • [مشاهده راهنمای نحوه ورود به سیستم • بازیابی کلمه‌عبور]
		۳۷	**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	-	۳۸	**FIA_UAU.5.1**	محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد: **[نام کاربری و کلمه عبور** **پیامک کلمه عبور یکبار مصرف]**
	-	۳۹	**FIA_UAU.5.2**	محصول باید هر کاربر متقاضی احرازهویت را مطابق زیر احراز هویت نماید: - **[کاربران از راه دور می توانند علاوه بر بررسی نام کاربری و کلمه عبور، از احراز هویت با استفاده از کلمه عبور ارسال شده از طریق پیامک که در بالا تحت عنوان کلمه عبور یکبار مصرف تعریف شده استفاده نمایند.]**
FIA_USB.1	- FIA_ATD.1	۴۰	**FIA_USB.1.1**	محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **شناسه کاربر** • **نقش های کاربر** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق)**
		۴۱	**FIA_USB.1.2**	محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید: • **زمانی‌که یک نشست جدید برقرار می‌شود، اطلاعات موجود از نشست-های قبلی باید حذف گردد** • **اطلاعات پیشینه احراز هویت باید بروزرسانی گردد** • **دسترسی کاربر به صفحات مختلف با توجه به نقش های کاربر بروزرسانی گردد.**
		۴۲	**FIA_USB.1.3**	محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: **هیچ تغییری در طول نشست فعال مجاز نمی‌باشد.**

۵-۱-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.1	- FMT_SMR.1 - FMT_SMF.1	۴۳	**FMT_MOF.1.1**	محصول باید توانایی تعیین رفتار کارکرد **های زیر** را به **مـدیر سیسـتم** محـدود نماید. • سرویس های پیامک • دسترسی کاربران به صفحات • نقش کاربران
FMT_MSA.1	- [FDP_ACC.1 or FDP_IFC.1] - FMT_SMR.1 - FMT_SMF.1	۴۴	**FMT_MSA.1.1**	محصول باید با اعمال **کنترل دسترسی کاربران به صفحات**، توانایی **انجام عملیـات های زیر را بر رو روی** مشخصه‌های امنیتی **ذکر شده** را به **مـدیر سیسـتم** محـدود نماید. شماره | مشخصه های امنیتی | توانایی ۱ | شناسه کاربر | پرس و جو و ویرایش ۲ | نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه | ویرایش ۳ | برخی جزئیات واسط کلاینت | تغییر پیش فرض
FMT_MSA.3	-	۴۵	**FMT_MSA.3.1**	محصول برای مشخصه‌های امنیتی که برای اعمال [**خط مشی**] استفاده مـی‌شـوند، بایـد مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.
		۴۶	**FMT_MSA.3.2**	محصول برای تعیین مقادیر اولیه پیشنهادی باید به [**مدیر سیستم**] اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد.
FMT_MTD.1	- FMT_SMR.1 - FMT_SMF.1	۴۷	**FMT_MTD.1.1 (1)**	محصول باید امکان [تغییـر، [**هیچ کارکرد دیگری**]] [**کلمه عبور همه کاربران**] را بـه

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[مدیر سامانه و هر کاربری که مجوز لازم را دارد] محدود نماید.
		۴۸	**FMT_MTD.1.1 (2)**	محصول باید توانایی [تغییر، [**هیچ کارکرد دیگری**]] [**کلمه عبور**] را به [**کاربر عادی**] محدود نماید.
FMT_SMF.1	-	۴۹	**FMT_SMF.1.1**	محصول باید قادر به انجام **کارکردهای مدیریتی که در جدول زیر آمده است** باشد:

مولفه استاندارد	مولفه	عملیات مدیریتی
FAU_SAR.1	بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
FAU_SEL.1	انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
FAU_STG.3	اقدامات لازم در زمان از دست رفتن داده ممیزی	• پشتیبانی از حدآستانه پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی حتمی ذخیره سازی ممیزی
FAU_STG.4	پیشگیری از اتلاف و از بین رفتن داده¬ ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
FDP_ACF.1	عملیات کنترل دسترسی ۱	مدیریت مشخصه های مورد استفاده برای ایجاد دسترسی و یا منع

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
			FDP_RIP.2	حفاظت از داده‌های باقیمانده ۲	انتخاب زمان اعمال حفاظت از اطلاعات باقی مانده (برای مثال به محض تخصیص یا حذف تخصیص) میتواند توسط هدف ارزیابی قابل پیکربندی باشد.
			FDP_ITC.2	ورود داده های کاربری به محصول ۴	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
			FDP_SDI.2	صحت داده های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می تواند قابل پیکربندی باشد.
			FIA_AFL.1	مدیریت احراز هویت ناموفق ۱	• مدیریت حدآستانه برای تلاش های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
			FIA_ATD.1	تعریف مشخصات کاربر ۱	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد، اگر در الزامات مشخص شده باشد.
			FIA_SOS.1	مدیریت کلمه عبور	مدیریت معیارها برای بررسی کلمه عبورها
			FIA_UAU.1	زمانبندی احراز هویت	• مدیریت داده احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
						توسط مدیر • مدیریت داده احرازهویت توسط کاربر مرتبط مدیریت لیست اقدامات قبل از اینکه کاربر احرازهویت شود
				FIA_UAU.5	سازوکار احرازهویت چندگانه	• مدیریت مکانیزم های احرازهویت مدیریت قوانین احرازهویت
				FIA_UID.1	شناسایی کاربر	• مدیریت شناسه های کاربر مدیریت لیست اقدامات اگر یک مدیر احرازشده بتواند اقدامات مجاز قبل از احرازهویت را تغییر دهد
				FIA_USB.1	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۱	• مدیر مجاز میتواند مشخصه های امنیتی موجودیت های فعال پیش فرض را تعریف کند. مدیر مجاز میتواند مشخصه های امنیتی موجودیت های فعال را تغییر دهد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				FMT_MOF.1	مدیریت رفتار توابع امنیتی	مدیریت گروهی از نقش هایی که با توابع امنیتی هدف ارزیابی در تعامل هستند.
				FMT_MSA.1	مدیریت مشخصه های امنیتی ۱	• مدیریت گروهی از نقش هایی که با مشخصه های امنیتی در تعامل هستند. مدیریت نقش هایی که مشخصه های امنیتی مقادیر معینی را به ارث میبرند.
				FMT_MSA.3	مدیریت مشخصه های امنیتی ۳	• مدیریت گروهی از نقش هایی که مقادیر اولیه را مشخص میکنند. • مدیریت تنظیمات محدودکننده و مجازکننده مقادیر پیش فرض برای سیاست های کنترل دسترسی مدیریت قوانینی که مشخصه های امنیتی مقادیر معینی را به ارث میبرند.
				FMT_MTD.1(1)	مدیریت داده های محصول ۱- مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده های توابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
						امنیتی هدف ارزیابی
				FMT_MTD.1(2)	مدیریت داده های محصول ۱- کاربرعادی، وارد کننده داده	مدیریت گروهی از قوانینی مرتبط با داده های توابع امنیتی هدف ارزیابی
				FMT_SMR.1	نقش های امنیتی ۱	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
				FTA_MCS.1	محدودیت بر روی چندین نشست همزمان	مدیریت حداکثر تعداد مجاز نشست های همزمان کاربران توسط مدیر
				FTA_SSL.3	قفل گذاری بر روی نشست‌ها و خاتمه دادن به آنها	• تعیین زمان غیرفعال بودن کاربر پس از آنکه پایان نشست برای هر کاربر روی داده است تعیین زمان پیش فرض غیرفعال بودن کاربر بعد از پایان نشست های تعاملی
				FTA_TSE.1	برقراری نشست ۱	مدیریت شرایط برقراری نشست توسط مدیر مجاز
FMT_SMR.1	- FID_UID.1	۵۰	**FMT_SMR.1.1**	نقش‌های زیر در محصول باید تعریف شده باشد: مدیر سامانه، کاربر عادی، دبیر دبیرخانه		

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۵۱	**FMT_SMR.1.2**	محصول، باید قادر به مرتبط نمودن کاربران با نقش‌های مجاز تعریف شده باشند.

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

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.1	-	۵۲	**FPT_FLS.1.1**	محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: **[شکست‌های نرم‌افزاری، شکست‌های کاربری]**
FPT_ITT.1	-	۵۳	**FPT_ITT.1.1**	محصول باید هنگام انتقال داده‌ها بین بخش‌های مجزای خود، در برابر افشاء یا تغییر محافظت نماید.
FPT_TDC.1	-	۵۴	**FPT_TDC.1.1**	محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [**شناسه کاربری و کلمه عبور**] را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد.
		۵۵	**FPT_TDC.1.2**	محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [**از الگوی امن برقراری ارتباط**] استفاده نماید.
FPT_TUD_EXT.1	-	۵۶	**FPT_TUD_EXT.1.2**	محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولید کننده محصول فراهم نماید که به‌روزرسانی نرم‌افزار و میان‌افزارمحصول مورد ارزیابی را به صورت دستی آغاز نماید و [از هیچ مکانیزم بروزرسانی پشتیبانی نمی کند].

۷-۱-۵- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.1	-	۵۷	**FRU_FLT.1.1**	محصول باید از عملکـرد [**تمام کارکردهای اصـلی**] هنگـام رویـداد شکسـت‌هـای زیـر اطمینان حاصل نماید: **[شکست نرم‌افزاری** **[هیچ شکست دیگر]]**

۸-۱-۵- کلاس دسترسی به هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_MCS.1	FIA_UID.1 -	۵۸	**FTA_MCS.1.1**	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.
		۵۹	**FTA_MCS.1.2**	محصول باید به صورت پیش‌فرض، **[۵ نشست همزمان پیش‌فرض]** برای هر کاربر در نظر بگیرد.
FTA_SSL.3	-	۶۰	**FTA_SSL.3.1**	محصول باید کلیه نشست‌های تعاملی راه دور[۴] را پس از مدت زمان **[۳۰ دقیقه]** غیرفعال بودن، خاتمه دهد.
FTA_SSL.4	-	۶۱	**FTA_SSL.4.1**	محصول باید اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.
FTA_TAH.1	-	۶۲	**FTA_TAH.1.1**	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست براساس **[روز، زمان و IP کاربر]** باشد.
	-	۶۳	**FTA_TAH.1.2**	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید [تاریخ] آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.
	-	۶۴	**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.

[4]Remote

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_TSE.1	-	۶۵	**FTA_TSE.1.1**	توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس [**مکان، شماره پورت، تعداد تلاش های ناموفق احرازهویت، شناسه کاربر(نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP، [هیچ مشخصه ی دیگر]]** ممانعت نماید.

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

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.1	-	۶۶	**FTP_TRP.1.1**	محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [TLS] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد.
	-	۶۷	**FTP_TRP.1.2**	محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.
	-	۶۸	**FTP_TRP.1.3**	محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی کند.
FTP_ITC.1	-	۶۹	**FTP_ITC.1.1**	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [TLS] میان خود و موجودیت IT معتبر، [**سرور ارسال پیامک**] 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.
		۷۰	**FTP_ITC.1.2**	محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.
		۷۱	**FTP_ITC.1.3**	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [**تمامی خدمات**] راه‌اندازی نماید.

۱۰-۱-۵- الزامات پیوست دو

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_HTTPS_EXT.1.	-	۷۲	**FCS_HTTPS_EXT.1.1**	محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.
		۷۳	**FCS_HTTPS_EXT.1.2**	محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.
		۷۴	**FCS_HTTPS_EXT.1.3**	درصورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید **برای برقراری اتصال درخواست مجوز نماید.**
FCS_TLSC_EXT.1	-	۷۵	**FCS_TLSC_EXT.1.1**	محصول باید TLS 1.2 (RFC5246) با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 هیچ مجموعه رمز دیگری
		۷۶	**FCS_TLSC_EXT.1.2**	محصول باید تأیید نماید که با توجه به RFC 6125، شناسه[5] ارائه‌شده با شناسه مرجع مطابقت داشته باشد.
		۷۷	**FCS_TLSC_EXT.1.3**	محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [ارتباط را برقرار نسازد].

[5] identifier

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۷۸	**FCS_TLSC_EXT.1.4**	محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های **secp256r1 و secp384r1** در پیام ClientHello ارائه دهد.
FCS_TLSS_EXT.1	-	۷۹	**FCS_TLSS_EXT.1.1**	محصول باید [انتخاب: (TLS 1.2 (RFC5246] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 هیچ مجموعه رمز دیگری]
		۸۰	**FCS_TLSS_EXT.1.2**	محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [TLS1.1] دارند، رد نماید.
		۸۱	**FCS_TLSS_EXT.1.3**	محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [۴۰۹۶ بیت] و [منحنی‌های NIST [secp256r1, secp384r1] و هیچ منحنی دیگری] ،[انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید.
FIA_X509_EXT.1	-	۸۲	**FIA_X509_EXT.1.1/Rev**	محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶.۳ تأیید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند: ○ گواهی‌نامه‌های مورداستفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing » (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند ○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف Client "Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.
	-	۸۳	**FIA_X509_EXT.1.2/Rev**	محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_X509_EXT.2	-	۸۴	**FIA_X509_EXT.2.1**	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای TLS و هیچ کاربرد دیگر از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.
		۸۵	**FIA_X509_EXT.2.2**	در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید گواهی را نپذیرد.

۶- توجیهات

۶-۱- الزامات پیاده سازی نشده

الزامات عملکردی زیر به دلایل ذکر شده در سامانه پیاده سازی نشده اند.

شماره المان	نام کلاس	نام مؤلفه	توضیحات
1	به روز رسانی امن ۳	FPT_TUD_EXT.1.3	در این سامانه از هیچ گونه بروزرسانی خودکار توسط پشتیبانی نمی شود. در صورت لزوم بروزرسانی توسط نماینده تولید کننده سامانه و تنها بر روی سرور سامانه انجام می شود.
2	**مهرهای زمانی**	FPT_STM.1.1	محصول مورد ارزیابی زمان را از سیستم عامل میزبان دریافت می‌نمایند و خود زمان را تولید و یا از time serverهای(ntp serverهای) معتبر دریافت نمی‌کنند

۷- الزامات تضمین امنیتی

الزامات امنیتی ذکر شده در این بخش مطابق با پروفایل حفاظتی کلاینت/سرور 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 آسیب‌پذیری
Life cycle Support	**ALC_CMC.1**	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۸- خلاصه مشخصات هدف ارزیابی

نسخه ۱.۴ سند هدف امنیتی نظام جامع پذیرش و بررسی پیشنهادات توسط شرکت نرم افزاری جادوی فکر تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

- محصول می تواند برای تمام رویدادهای ورود و خروج کاربر به/ از سیستم رکورد ممیزی تولید نماید و برای هر رکورد ممیزی، حداقل اطلاعات تاریخ و زمان رویداد، نام کاربری، IP کاربر، نوع و نسخه مرورگر مورد استفاده، صفحه ارجاع دهنده با سامانه و اولین صفحه مشاهده شده را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند. (FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1)
- محصول می تواند تمام رویدادهایی که توسط مدیر سامانه انتخاب شده را ممیزی نماید و برای هر رکورد ممیزی، حداقل اطلاعات تاریخ و زمان رویداد، کد کاربری، نوع عملیات و توضیحات عملیات را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند. امکان مشاهده رویدادهای ثبت شده هر کاربر برای خود کاربر وجود دارد. امکان مشاهده همه رویدادها برای ممیز سامانه وجود دارد. (FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_SAR.3.1, FAU_SEL.1.1)
- از طریق خود نرم افزار امکان حذف یا ویرایش غیر مجاز داده ممیزی وجود ندارد. کاربر تنها در صورتی امکان حذف یا ویرایش داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات مورد نظر خود را انجام دهد. در صورت ویرایش غیر مجاز داده های ممیزی، رکوردهای ویرایش شده با استفاده از ستون Hash تعبیه شده قابل تشخیص خواهند بود. (FAU_STG.1.1, FAU_STG.1.2)
- در صورتی که حجم داده های ممیزی از محدوده اول تعیین شده توسط مدیر سامانه بیشتر شود به مدیر سامانه از طریق پیامک هشدار داده می شود و در صورتی که حجم داده ممیزی از محدوده دوم تعیین شده توسط مدیر سامانه بیشتر شود علاوه بر هشدار به مدیر سامانه توسط پیامک، سامانه شروع به حذف از قدیمی ترین داده های ممیزی می کند. حدود اول و دوم و مقدار داده های قدیمی که در این حالت حذف می شوند توسط مدیر سامانه در صفحه تنظیمات امنیتی قابل تنظیم است (مقدار قابل قبول ۱ تا ۵۰ درصد است). چک نمودن محدود حجم داده های ممیزی هر بار در زمان ثبت ممیزی جدید انجام می شود اما ارسال پیام برای عبور از محدوده اول تعیین شده تنها روزی یکبار انجام می شود. (FAU_STG.3.1, FAU_STG.4.1)
- محصول مقدار هش شده اطلاعات در جداول حساس را جهت صحت اطلاعات با استفاده از الگوریتم درهمسازی SHA1 در خود جداول ذخیره می نماید و از همین الگوریتم جهت بررسی صحت اطلاعات استفاده می نماید تا بتوان از صحت اطلاعات اطمینان حاصل نمود. باید توجه نمود که مقدار هش تولید شده از مقدار موجود در همه ستون های جدول نبوده و در برخی موارد با توجه به عدم اهمیت اطلاعات از بکارگیری برخی از آنها در الگوریتم هش صرف نظر شده است. لیست جداولی که در آنها از هش جهت بررسی صحت اطلاعات استفاده شده و فیلدهایی که در محاسبه هش استفاده شده اند به شرح ذیل است: (FCS_COP.1.1(1), FCS_COP.1.1(2))

نام جدول	نام فیلدهایی که در محاسبه هش استفاده شده اند
personnel	Code - Fname - Lname - Name - Code_r - Code_mad - Sabgh - Jens - Phon - Code_vsz - Code_m - Code_sh - Email - Shogl - Addr - post10 - UserName - PersonnelActiveStatusId - PersonnelStatusId - Mobile - TributarySecretariatID - OrganizationStructureLevel1ID - OrganizationStructureLevel2ID - OrganizationStructureLevel3ID - EmploymentDate - UpdatingStatusFromPersonnelSystem - IsInternalPersonnel -

UserIP - PersonnelFormViewOrderField - IsPasswordChanged - IsRequiredFieldsUpdated - IsVirtual - PersonnelCode - BankingCardNumber - BankingCardExporterBank - SpecialDesc - StaffLevelId - ActivityAreaId - OrganizationStructureLevel4ID - SazmanId - AutomationUserName - Ostanid - Cityid - BirthDayDate - Code_mvn - TypeShrktID - CreateDatePerson	
ApplicationId - RoleId - RoleName - LoweredRoleName - Title - Description	**aspnet_roles**
ActionName - UserRoleId	**aspnet_userroleactions**
ApplicationId - UserId - UserName - LoweredUserName - MobileAlias - IsAnonymous	**aspnet_users**
UserId - RoleId	**aspnet_usersinroles**
ApplicationId - UserId - Password - PasswordFormat - PasswordSalt - MobilePIN - Email - LoweredEmail - PasswordQuestion - PasswordAnswer - IsApproved - IsLockedOut - CreateDate - LastLoginDate - LastPasswordChangedDate - LastLockoutDate - FailedPasswordAttemptCount - FailedPasswordAttemptWindowStart - FailedPasswordAnswerAttemptCount - FailedPasswordAnswerAttemptWindowStart - Comment	**aspnet_membership**
TributarySecretariatResponsibleID - TributarySecretariatID - ResponsibleID	**tributarysecretariattesponsible**
CommitteeSecretaryID - CommitteeID - PersonnelID - IsActive	**Committeesecretary**
KarshenasiGroupID - Name - SecretaryID - TributarySecretariatID - IsActive - ViewOrder	**karshenasigroup**
AuditId - IsActive	**audit**
CentralSecretariatId - IsActive	**centralsecretariat**
CentralSecretariatExecuterID - IsActive	**centralsecretariatexecuter**

- محصول امکان تنظیم حداقل تعداد حروف و نوع حروفی که باید در کلمه عبور استفاده شود را در اختیار مدیر سامانه قرار داده است تا بتوان از این طریق میزان سختی کلمه های عبور را مدیریت نمود. این تنظیمات در صفحه تنظیمات امنیتی وجود دارد. (FIA_PMG_EXT.1.1)
- می توان با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد. زمانی که تعداد تلاش ناموفق کاربر به عدد تعیین شده رسید حساب کاربری قفل می شود. تنظیمات مربوط به این بخش در صفحه تنظیمات امنیتی قرار گرفته است. (FIA_AFL.1.1, FIA_AFL.1.2)
- پیش از ورود کاربر به محصول، پنجره ورود در اختیار کاربر است تا از این طریق روال ورود به او آموزش داده شود. سایر عملیات مستلزم شناسایی و احراز هویت کاربر خواهد بود. (FIA_UAU.1.1, FIA_UAU.1.2)
- محصول علاوه بر احراز هویت توسط نام کاربری و کلمه عبور، امکان احراز هویت دو مرحله ای از طریق ارسال پیامک را نیز فراهم می نماید. (FIA_UAU.5.1, FIA_UAU.5.2)
- محصول مشخصه‌های امنیتی شناسه کاربر داده های احراز هویت، نقش کاربر، وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)، IP کاربر، رمز عبور کاربر و ایمیل کاربر را برای هر کاربر نگهداری می کند. (FIA_ATD.1.1)

- زمانیکه یک نشست جدید برقرار می شود، اطلاعات موجود از نشست های قبلی حذف میگردد. اطلاعات پیشینه احراز هویت بروزرسانی میشود. رکورد ممیزی برای ورود کاربر در نشست جدید ثبت میگردد. در این رکورد اطلاعات کاربر که شامل نام کاربری، زمان ورود و جزئیات واسط کاربری است ذخیره می شود. همچنین برای کاربری اطلاعاتی در خصوص آخرین احراز هویت موفق و ناموفق با نام کاربری او نمایش داده می شود. (FIA_USB.1.1, FIA_USB.1.2, FIA_USB.1.3)
- در زمان ارسال درخواست کاربر به سمت سرور، دسترسی کاربر به صفحه مربوطه چک می شود، همچنین در صورتی که در درخواست ارسالی فایلی ضمیمه شده باشد، محتوای آن توسط آنتی ویروس مورد ارزیابی قرار می گیرد.((FDP_ITC.2.1, FDP_ITC.2.2, FDP_ITC.2.3, FDP_ITC.2.4, FDP_ITC.2.5))
- در زمان درخواست دریافت خروجی از سامانه اطلاعات با توجه به دسترسی های کاربر دریافت شده و تنها امکان خروج اطلاعاتی وجود دارد که مدیر سامانه مشخص کرده است. (FDP_ETC.2.1, FDP_ETC.2.2, FDP_ETC.2.3, FDP_ETC.2.4)
- جداول حساس سامانه دارای ستون هش است که مقدار آن درهم سازی شده داده های آن رکورد است که محصول از طریق آنها صحت اطلاعات را بررسی می نماید. محصول به صورت خودکار ساعت ۱۱ هر شب صحت داده های حساس سامانه را از طریق ستون hash مورد بررسی قرار داده و در صورت وجود عدم تطابق، خلاصه ای از موارد عدم انطباق را در صفحه میزکار مدیر سامانه نمایش می دهد. در صفحه اطلاعات دستکاری شده (که مدیر سامانه از طریق منوی مدیر سیستم -> مدیریت کاربران -> اطلاعات دستکاری شده می تواند به آن دسترسی داشته باشد) ریز اطلاعاتی که مقادیر آنها با مقدار hash تطابق ندارد نمایش داده می شود. همچنین در صفحه اطلاعات دستکاری شده امکان بررسی دستی صحت اطلاعات وجود دارد تا کاربر هر زمانی که نیاز بود از آن استفاده نماید. (FDP_SDI.2.1, FDP_SDI.2.2)
- محصول دسترسی به صفحات را با توجه به نام کاربری و نقش کاربر مدیریت می کند و از این طریق دسترسی کاربر به داده ها و عملیات را نیز مدیریت می نماید. (FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3)
- محصول می تواند با توجه به تنظیماتی که توسط مدیر سامانه انجام می شود، از ورود کاربرانی که تعداد درخواست ورود آنها بیش از حد مجاز بوده جلوگیری نماید. همچنین ورود کاربرانی که تعداد نشست های جاری آنها بیش از حد مجاز است امکان ورود به محصول را نخواهند داشت. (FDP_ACF.1.4)
- در زمان خروج کاربر از سامانه همه منابع اختصاص داده شده به کاربر آزاد سازی شده و جهت دسترسی مجدد به اطلاعات باید مجددا اعتبارسنجی انجام شود. (FDP_RIP.2.1)
- امکان تغییر پارامترهای مربوط به سرویس های پیامک تنها در اختیار مدیر سامانه است. همچنین تغییراتی که موجب ویرایش نقش کاربران می شود تنها در اختیار مدیر سامانه است. علاوه بر این تنها مدیر سامانه است که می تواند دسترسی هر یک از کاربرها را به صورت انفرادی تغییر دهد. (FMT_MOF.1.1)
- تنها مدیر سامانه توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را دارد. همچنین تنها مدیر سامانه می تواند اطلاعات کاربران، نقش ها و دسترسی کاربران را حذف و ویرایش نماید. مدیر سامانه امکان ایجاد کلمه عبور جدید برای همه کاربران دارد و هر کاربر تنها می تواند کلمه عبور خود را در صفحه تغییر اطلاعات کاربری تغییر دهد. (FMT_MSA.1.1, FMT_MTD.1.1, FMT_MSA.3.1, FMT_MSA.3.2)

- محصول این امکان را به مدیر سامانه می دهد تا کارکردهای امنیتی سامانه را از طریق اعمال تنظیمات در بخش های مختلف مدیریت نماید. (FMT_SMF.1.1)
- نقش های مورد نیاز محصول (مانند: مدیر سامانه، کاربر عادی، دبیر دبیر کمیته و ...) به صورت پیش فرض در آن ایجاد شده است. مدیر سامانه می تواند کاربران مجاز را با توجه به روال کاری آنها به هر یک از این نقش ها مرتبط سازد. (FMT_SMR.1.1, FMT_SMR.1.2)
- در زمانی که محصول به هر دلیلی (نرم افزاری یا کاربری) دچار مشکل شود، وضعیت امن خود را حفظ می نماید. (FPT_FLS.1.1)
- محصول در زمان ارتباط با محصول های IT دیگر از مکانیزم های امنیتی مانند توکن یا نام کاربر و کلمه عبور (با توجه به ارائه دهنده سرویس) برای ارسال و دریافت اطلاعات استفاده می نماید تا صحت هویت فرستنده یا گیرنده تایید شود و امنیت اطلاعات در زمان ارسال و دریافت حفظ باشد. (FPT_TDC.1.1, FPT_TDC.1.2)
- محصول دارای هیچگونه روال بروزرسانی خودکار نمی باشد و بروزرسانی توسط کارشناس شرکت تولید کننده و با اتصال به سرور سامانه انجام می شود. (FPT_TUD_EXT.1.2)
- بخش های مجزای محصول شامل پایگاه داده، خود نرم افزار(که بر روی سرور در حال اجرا است) و رابط کاربری (که توسط مرورگر اجرا می شود) است. رابط کاربری ارتباط مستقیم با پایگاه داده ندارد. ارتباط بین رابط کاربری و نرم افزار محصول توسط پروتکل https انجام شده و به صورت رمزنگاری شده انجام می گردد. ارتباط بین نرم افزار و پایگاه داده نیز توسط نام کاربری و کلمه عبوری که بر روی پایگاه داده تنظیم شده است اعتبار سنجی می شود.(FPT_ITT.1.1)
- محصول تعداد نشست های فعال هم زمان کاربر را محدود به تعدادی می کند که توسط مدیر سامانه تعیین می شود و مقدار پیش فرض آن ۵ نشست است. (FTA_MCS.1.1, FTA_MCS.1.2)
- کاربر این امکان را دارد تا نشست مورد نظر خود را به صورت دستی خاتمه دهد. همچنین کلیه نشست های فعال پس از مدت ۳۰ دقیقه (قابل تنظیم توسط توسعه دهنده و پشتیبان سامانه) عدم استفاده خاتمه می یابد. (FTA_SSL.3.1, FTA_SSL.4.1)
- در صورت برقراری نشست به طور موفقیت آمیز، محصول این موارد را جهت اطلاع کاربر به او نمایش می دهد: - آخرین تلاش موفق برای ایجاد نشست براساس روز، زمان و IP. - زمان آخرین تلاش ناموفق که بعد از تلاش موفق قبلی انجام شده است. - تعداد تلاش های ناموفقی که در بازه تلاش موفق قبلی تا کنون برای ورود به این حساب کاربری انجام شده است. (FTA_TAH.1.1, FTA_TAH.1.2)
- کاربر می تواند هر زمان که خواست لیست کامل دسترسی های خود را مشاهده نماید. در این لیست تنها امکان مشاهده وجود دارد و امکان حذف و ویرایش به کاربر داده نشده است. (FTA_TAH.1.3)
- محصول این امکان را دارد تا با اعمال تنظیمات توسط مدیر سامانه، از برقراری نشست برای کاربرانی با IP خاص و در زمان خاص ممانعت نماید. همچنین مدیر سامانه می تواند با اعمال تنظیمات از ورود[۶] کاربرانی که از تعداد مشخصی کلمه عبور را اشتباه وارد نموده اند ممانعت به عمل آورد. علاوه بر این مدیر سامانه

[۶] Login

می تواند هر یک از کاربران مورد نظر خود را غیر فعال نماید تا امکان ورود به سامانه برای کاربر مورد نظر وجود نداشته باشد. (FTA_TSE.1.1)

- محصول می تواند مسیر ارتباطی امنی را با استفاده از پروتکل HTTPS میان خود و هرموجودیت IT دیگر فراهم نماید (در صورتی موجودیت مورد نظر از ارتباط امن پشتیبانی نماید) تا آنها را احراز هویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند و تمامی بخش های سیستم، سازگاری کامل با پروتکل های امن SSL و غیره را دارند. (FTP_ITC.1.1, FTP_ITC.1.3)
- محصول می تواند مسیر ارتباطی امنی را با استفاده از پروتکل HTTPS میان خود و مدیر سامانه فراهم نماید تا آنها را احراز هویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند به مدیر سامانه اجازه دهد که ارتباط را از طریق کانال امن آغاز کند و تمامی بخش های سیستم، سازگاری کامل با پروتکل های امن SSL و غیره را دارند. (FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3)
- برقراری ارتباط بین کاربر و سامانه از طریق پرتکل https و با استفاده از TLS انجام می شود و در صورتی که گواهی https در زمان برقراری ارتباط معتبر نباشد کاربر با توجه به مرورگری که از آن استفاده می کند با پیامی مواجه می شود که نشان دهنده عدم اعتبار گواهی است و برای ادامه کار با شرایط جاری باید با کلیک بر روی دکمه مربوطه اطلاع از شرایط را تایید نماید. (FCS_HTTPS_EXT.1.1, FCS_HTTPS_EXT.1.2, FCS_HTTPS_EXT.1.3)
- زمانی که کاربر راه دور درخواست ارتباط با محصول را داشته باشد و یا محصول درخواستی را به سمت کاربر یا سامانه دیگری ارسال می نماید، محصول تنها از پروتکل ها و الگوریتم های رمزنگاری امن در زمان برقراری ارتباط و ارسال اطلاعات استفاده می نماید و درخواست هایی که از پروتکل ها و الگوریتم های امن پشتیبانی نمی کنند را رد می نماید. این تنظیمات در سرور نرم افزار اعمال شده و تنها پروتکل ها و الگوریتم های رمزنگاری قابل قبول فعال هستند. در خود نرم افزار نیز تنظیم شده است تا ارتباط تنها از طریق TLS 1.2 انجام شود. (FCS_TLSC_EXT.1.1 , FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.1.3, FCS_TLSC_EXT.1.4, FCS_TLSS_EXT.1.1, FCS_TLSS_EXT.1.2, FCS_TLSS_EXT.1.3)
- محصول در زمان برقراری ارتباط امن با سرورهای دیگر مانند سرور ارسال پیامک، برای مدیریت و اعتبارسنجی گواهی نامه های CA از استاندارد X509 استفاده می نماید. این اعتبار سنجی به صورت خودکار توسط «Net Framework.» انجام می شود. در مکانیز پیشفرض این چهارچوب برای چک نمودن revocation از مکانیزم CRL (Certificate Revocation List) استفاده شده است. در صورتی که اعتبار سنجی گواهی نیاز به اطلاعات اضافه داشته باشد و امکان برقراری ارتباط وجود نداشته باشد از برقراری ارتباط جلوگیری می شود. (FIA_X509_EXT.1.1/Rev, FIA_X509_EXT.1.2/Rev, FIA_X509_EXT.2.1, FIA_X509_EXT.2.2)