به نام خدا

سند هدف امنیتی سامانه مدیریت نامگذاری معابر و اماکن شهری (منام)-نسخه 2.2.1

مدرن اندیشان ساعی

شهریور-1400

نسخه 1.5

فهرست

خواهشمند است در هنگام تدوین سند عبارات مشخص شده با [ ] تکمیل نموده و کروشه را حذف نمائید.

1- معرفی سند هدف امنیتی

1-1- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سامانه مدیریت نامگذاری معابر و اماکن شهری (منام)
نسخه	1.5
تاریخ	31 شهریور 1400
نویسندگان	گروه ساعی

1-2- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	مدرن اندیشان ساعی
نام محصول	سامانه مدیریت نامگذاری معابر و اماکن شهری (منام)
نوع محصول	نرم افزار تحت شبکه مبتنی بر اطلاعات جغرافیایی
نسخه	2.2.1

1-3- مرور کلی هدف ارزیابی

1-3-1- توابع امنیتی اصلی هدف ارزیابی

با توجه به گسترش روز افزون استفاده از سامانه‌های اطلاعاتی به منظور تسهیل در فرآیندهای کسب و کار، ضروری است تا کمیسیون‌های نامگذاری معابر و اماکن شهری، از اینگونه سامانه‌ها به منظور مکانیزه نمودن فرآیندهای خود استفاده نمایند. از آنجاییکه امروزه کاربرد سامانه‌های اطلاعات جغرافیایی، رو به گسترش می‌باشد، لذا شرکت ساعی در سامانه مدیریت نامگذاری معابر و اماکن شهری، از قابلیت‌های مکانی به منظور کارآمدتر و جذاب‌تر نمودن فرآیندهای کمیسیون‌های نامگذاری معابر و همچنین پیاده‌سازی انواع تحلیل‌های مکانی، استفاده نموده است.

این سامانه برپایه سیستم RBAC (سیستم مبتنی بر نقش کاربران) می‌باشد که در آن نقش‌های گوناگونی تعریف می‌گردد. به گونه‌ای که هر نقش شامل یک سری دسترسی هایی است که به کاربر اجازه می‌دهد تا به بخشی از سیستم دسترسی داشته باشد. هر کاربر در این سیستم می‌تواند یک و یا چند نقش متفاوت داشته باشد و بر اساس آن نقش‌ها و دسترسی‌های تعریف شده، درون هر نقش به قسمتی از سیستم دسترسی داشته باشد.

2-3-1- نوع هدف ارزیابی

نرم افزار تحت شبکه مبتنی بر اطلاعات جغرافیایی

3-3-1- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

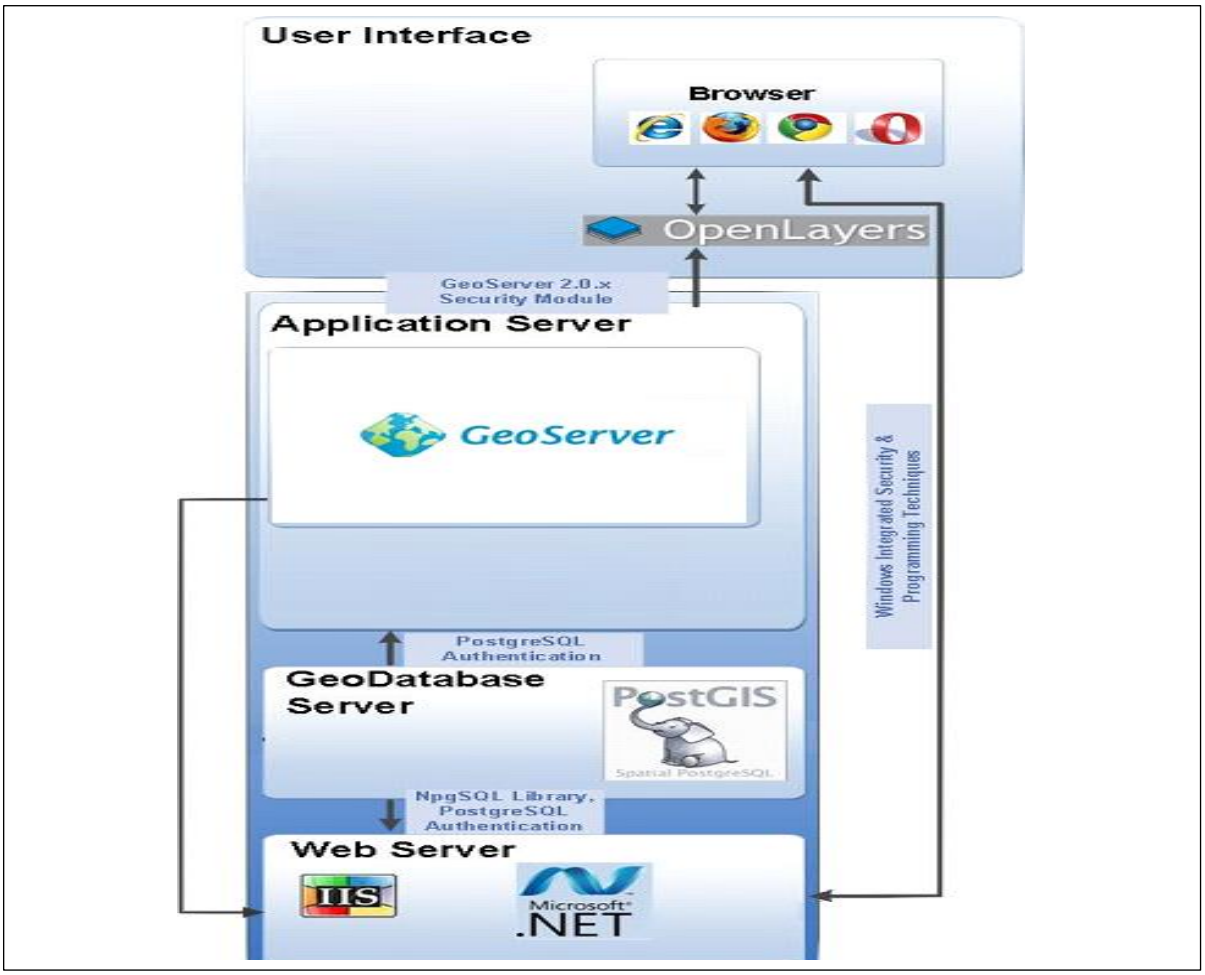
در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

کامپوننت‌ها	حداقل الزامات
پردازنده	Quad core 2.5GHZ +
حافظه	حداقل GB8
فضای آزاد	500GB
سیستم عامل	Windows server 2008 R2 به بالا
DBMS	Postgresql 13.0 +
زبان برنامه نویسی	ASP.NET , C#
نرم افزار لازم	.NET Framework 4.5 IIS

4-1- توصیف هدف ارزیابی

1-4-1- حوزه فیزیکی

عناصر محصول	شماره مدل یا نسخه
نرم افزار GeoServer	نسخه 2.18.1
نرم افزار Postgis Extension	نسخه 3.0
نرم افزار pgAdmin	نسخه 4
ابزار Openlayers	نسخه 2



2-4-1- حوزه منطقی

کارکردها	توصیف
ورود با استفاده از نام کاربری و رمز عبور	کاربر با استفاده از نام کاربری و رمز عبور می‌تواند به سیسم وارد شود که این اطلاعات توسط مدیر سیستم تعریف می‌شود. قبل از ورورد کاربر نمیتواند عملیاتی را انجام دهد و حتما باید توسط سامانه شناسایی شود.
قفل شدن کاربر درصورت وارد کردن مکرر رمز اشتباه	در صورتی که کاربر رمز عبور را اشتباه وارد نماید(5 بار. این مقدار توسط مدیر قابل تغییر میباشد) امکان ورود به سیستم از آن کاربر گرفته می‌شود(قفل می‌شود). مدیر سیستم می‌تواند کاربر را مجددا فعال نماید.
جلوگیری از عبارات غیرمجاز	در صورتی که کاربر اطلاعات غیر مجاز(injection) وارد کند، به منظور حفظ امنیت اطلاعات،سیستم از ثبت اطلاعات جلوگیری و به کاربر هشدار می‌دهد
مدیریت کاربر مبتنی بر نقش	دسترسی همه کاربران در سامانه توسط مدیر به واسطه نقش/ها تعریف می‌شود و فقط اطلاعاتی را می‌توانند مشاهده،ثبت و حذف نمایند که به آنها

کارکردها	توصیف
	دسترسی داشته باشند. مدیر میتواند نقش را به کاربر اختصاص یا آن نقش را حذف کند.
رمزنگاری رمز عبور	رمز عبور ذخیره شده به دلیل حفظ امنیت، در سیستم به صورت الگوریتم sha-384 رمزنگاری می‌شود و قابل بازیابی توسط هکر نمیباشد. زیرا از درهم سازی مناسبی برخوردار است
ورود دو مرحله‌ای	سامانه قابلیت ورود دو مرحله‌ای را برای کاربر فراهم میکند. به این صورت که یک کد یکتا به شماره تلفن کاربر ارسال میشود و در صورت وارد کردن کد صحیح توسط کاربر در سامانه، به سیستم وارد میشود
کنترل شدن فعالیت کاربران	فعالیت تمامی کاربران در طول کار با سیستم ردیابی و ذخیره میشود. این منظور باعث میشود مدیر رفتار کاربران را شناسایی کرده و از انجام عملیات غیر مجاز آگاه شود.

2- ادعای انطباق

2-1- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استلندارد ارزیابی امنیتی معیار مشترک	ISO/IEC 15408, version 3.1, revision 5, April 2017
انطباق با SFRها (قسمت دوم از CC)	توسعه یافته
انطباق با SARها (قسمت سوم از CC)	منطبق

2-2- انطباق با پروفایل حفاظتی

نام پروفایل حفاظتی	این سند هدف امنیتی به پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه، نسخه 1.1 ، اسفند 96 انطباق دارد

2-3- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	این سند هدف امنیتی به سطح EAL1 انطباق دارد

3- تعریف مسائل امنیتی

3-1- خط‌مشی

عنوان فارسی خط‌مشی	عنوان انگلیسی خط‌مشی	توصیف
ممیزي کامل	P.COMPLEMENTARY_AUDIT	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می‌گیرند.
پیکربندی مناسب	P.PROPER_CONFIGURATION	پیکربندی پیش‌فرض محصول و مولفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش‌فرض، خطاهای پیش‌فرض و صفحات 404، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خط‌مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	P.E_SIGNATURE	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

عنوان فارسی خطمشی	عنوان انگلیسی خطمشی	توصیف
ارتباط امن	P.SSL_COMMUNICATION	در صورت فراهم بودن زیرساخت برای ارتباط امن، سیستم به درستی اطلاعات را رد و بدل میکند

2-3- تهدیدات

عنوان فارسي تهديد	عنوان انگلیسی تهدید	توصیف
دسترسي غيرمجاز	T.UNAUTHORIZED_ACCESS	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. 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 باقیملنده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تولند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
		رکوردهای، مستندات و داده‌های حفاظت شده توسط محصول می‌تواند

عنوان فارسي تهديد	عنوان انگليسی تهديد	توصيف
تغییر غیرمجاز	T.DATA_ALTERATION	بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نمی‌باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	T.REPUDIATION	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می‌باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشاي اطلاعات	T.DATA_DISCLOSURE	داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می‌تواند عمداً یا غیر

عنوان فارسي تهديد	عنوان انگليسی تهديد	توصيف
		عمد موجب افشـــاء اطلاعات محرمانه گردد.
انكار سرويس	T.DENIAL_OF_SERVICE	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.
داده‌هاي ورودي مخرب	T.HARMFUL_DATA	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.
دسترسي غيرمجاز	T.ELEVATION_OF_PRIVILEGES	مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یلبد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.
		در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد

عنوان فارسي تهديد	عنوان انگلیسی تهدید	توصیف
شنود شبکه	T.NETWORK_EAVESDROP	موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده‌های رد و بدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال می‌توان به موردی اشاره کرد که در آن یک کاربر تلاش می‌کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می‌نماید.

3-3-

فرضیات

عنوان فرضیه فارسی	عنوان فرضیه انگلیسی	توصیف
پشتیبان گیری مناسب	A.PROPER_BACKUP	تمامی داده‌های موجود در سیستم در بازه زمانی مشخص دارای پشتیبان مناسبی هستند که در صورت حذف شدن داده‌ها، امکان بازیابی آن‌ها وجود دارد
محیط امن	A.SECURE_ENVIRONMENT	دسترسی غیر مجاز به محیط کاری به طور مناسب محدود شده است.
ارتباطات	A.COMMUNICATION	فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.
تحویل امن	A.SECURE_DELIVERY	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.

عنوان فرضیه فارسی	عنوان فرضیه انگلیسی	توصیف
انکار سرویس توزیع شده	A.DIST_DENIAL_OF_SERVICE	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.
کاربران آموزش دیده	A.TRUSTED_ADMIN	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
توسعه دهندگان آموزش دیده	A.TRUSTED_DEVELOPER	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند.
توسعه دهندگان مجرب	A.EXPERIENCED_DEVELOPER	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.

4- اهداف امنیتی

4-1- اهداف امنیتی برای هدف ارزیابی

عنوان اهداف امنیتی برای هدف ارزیابی به زبان فارسی	عنوان اهداف امنیتی برای هدف ارزیابی به زبان انگلیسی	توصیف
احراز هویت	O.AUTH	سامانه کاربر را ملزم به استفاده از رمز عبور قدرتمند می‌کند. پس از ورود به سیستم، سامانه کاربر را تشخیص داده و اطلاعات را متناسب با نقش اختصاص یافته به کاربر نمایش می‌دهد.
کنترل جریان داده	O.DATA_FLOW_CONTROL	سامانه داده‌ها غیر مجاز را شناسایی و از ثبت آنها جلوگیری می‌کند

عنوان اهداف امنیتی برای هدف ارزیابی به زبان فارسی	عنوان اهداف امنیتی برای هدف ارزیابی به زبان انگلیسی	توصیف
مدیریت	O.MANAGEMENT	مدیر سیستم می‌تواند به صورت کامل ، کارکردهای کاربران را مشاهده کند. همچنین سیستم قابلیت تغییر مجوزها(دسترسی) را برای مدیر فراهم می‌سازد
مدیریت خطا	O.ERROR_MANAGEMENT	سامانه خطاهای رخ داده هنگام عملیات را به طور معنا دار نمایش می‌دهد برای مثال هنگام ورود داده غیر مجاز ، پیغام "عدم ورود داده مجاز" نمایش داده می‌شود
ارتباطات امن مبتنی بر TLS	O.SSL_COMMUNICATION	سامانه در صورت نیاز، به درستی از طریق پروتکل ارتباطی TLS استفاده می‌کند و باعث بروز اختلال در سامانه نمی‌شود
ممیزی	O.AUDIT	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه نماید.
صحت داده	O.DATA_INTEGRITY	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت داده‌های باقیمانده	O.RESIDUAL_DATA_MNG	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می‌گردد.

2-4- اهداف امنیتی برای محیط عملیاتی

عنوان اهداف امنیتی برای محیط عملیاتی به زبان فارسی	عنوان اهداف امنیتی برای محیط عملیاتی به زبان انگلیسی	توصیف
محیط امن	OE.SECURE_ENVIRONMENT	امنیت فیزیکی نسبتا خوبی برقرار است تا ارزش دارایی‌ها تا حد ممکن حفظ شود
ارتباطات	OE.COMMUNICATION	ارتباط امن بین محیط عملیاتی و محصول برقرار می‌باشد
کاربران آموزش دیده	OE.TRUSTED_ADMIN	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان آموزش دیده	OE.TRUSTED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان مجرب	OE.EXPERIENCED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده‌ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.
ممیزی کامل	OE.COMPLEMENTARY_AUDIT	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می‌باشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	OE.SECURE_DELIVERY	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا

عنوان اهداف امنیتی برای محیط عملیاتی به زبان فارسی	عنوان اهداف امنیتی برای محیط عملیاتی به زبان انگلیسی	توصیف
		پارامترهای استفاده شده به منظور تست باید پاک یا غیر قابل دسترس گردند.
پشتیبان‌گیری مناسب	OE.PROPER_BACKUP	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال‌های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

5- نیازمندی‌های امنیتی

5-1- الزامات کارکرد امنیتی

در سند جاری کلیه عملگرهای انتخاب به صورت زیرخطدار و عملگرهای اختصاص به صورت بولد نوشته شده اند و براکت ها نیز برای عملگرها لحاظ شده است.

عملگرهای تکرار در داخل پرانتز و بعد از شناسه‌ی الزام مشخص می‌شوند. به عنوان مثال FCS_COP.1.1(1) و FCS_COP.1.1(2) نشانگر عملگر تکرار بر روی الزام FCS_COP.1.1 هستند.

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
1	ممیزی امنیت	**تولید داده ممیزی 1**	FAU_GEN.1.1
2		**تولید داده ممیزی 2**	FAU_GEN.1.2
3		**بازبینی داده ممیزی 1**	FAU_SAR.1.1
4		**بازبینی داده ممیزی 2**	FAU_SAR.1.2
5		**بازبینی داده ممیزی محدود 1**	FAU_SAR.2.1
6		**بازبینی داده ممیزی قابل انتخاب 1**	FAU_SAR.3.1
7		**ذخیره‌سازی رویدادهای ممیزی 1**	FAU_STG.1.1
8		**ذخیره‌سازی رویدادهای ممیزی 2**	FAU_STG.1.2
9		**انتخاب داده ممیزی 1**	FAU_SEL.1.1
10		**اقدامات لازم در زمان از دست رفتن داده ممیزی 1**	FAU_STG.3.1
11		**پیشگیری از اتلاف و از بین رفتن داده ممیزی 1**	FAU_STG.4.1
12		**مرتبط نمودن هویت کاربر به رویداد 1**	FAU_GEN.2.1
13	پشتیبانی از رمزنگاری	**عملیات رمزنگاری 1 (1) (یکپارچگی داده‌های رکورد و داده‌های ممیزی)**	FCS_COP.1.1(1)
14		**عملیات رمزنگاری 1 (2) (تولید مقادیر hash)**	FCS_COP.1.1(2)
15		**الزامات پروتکل HTTPS (1)**	FCS_HTTPS_EXT.1.1
16		**الزامات پروتکل HTTPS (2)**	FCS_HTTPS_EXT.1.2

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
17		الزامات پروتکل HTTPS (3)	FCS_HTTPS_EXT.1.3
18		الزامات پروتکل TLS Client (1)	FCS_TLSC_EXT.1.1
19		الزامات پروتکل TLS Client (2)	FCS_TLSC_EXT.1.2
20		الزامات پروتکل TLS Client (3)	FCS_TLSC_EXT.1.3
21		الزامات پروتکل TLS Client (4)	FCS_TLSC_EXT.1.4
22		الزامات پروتکل TLS Server (1)	FCS_TLSS_EXT.1.1
23		الزامات پروتکل TLS Server (2)	FCS_TLSS_EXT.1.2
24		الزامات پروتکل TLS Server (3)	FCS_TLSS_EXT.1.3
25		الزامات پروتکل TLS Server/ احرازهویت (4)	FCS_TLSS_EXT.2.4
26		الزامات پروتکل TLS Server/ احرازهویت (5)	FCS_TLSS_EXT.2.5
27		الزامات پروتکل TLS Server/ احرازهویت (6)	FCS_TLSS_EXT.2.6
28	حفاظت از داده کاربری	خط‌مشی کنترل دسترسی 1	FDP_ACC.1.1
29		عملیات کنترل دسترسی 1	FDP_ACF.1.1
30		عملیات کنترل دسترسی 2	FDP_ACF.1.2
31		عملیات کنترل دسترسی 3	FDP_ACF.1.3
32		عملیات کنترل دسترسی 4	FDP_ACF.1.4
33		حفاظت کامل از اطلاعات باقیمانده در منابع 1	FDP_RIP.2.1
34		صحت داده کاربری ذخیره شده 2	FDP_SDI.2.1
35		صحت داده کاربری ذخیره شده 3	FDP_SDI.2.2
36	شناسایی و احراز هویت	شناسایی کاربر 1	FIA_UID.1.1
37		شناسایی کاربر 2	FIA_UID.1.2
38		مدیریت احرازهویت ناموفق 1	FIA_AFL.1.1
39		مدیریت احرازهویت ناموفق 2	FIA_AFL.1.2
40		تعریف مشخصات کاربر 1	FIA_ATD.1.1
41		مدیریت کلمه عبور	FIA_PMG_EXT.1.1

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
42		احرازهویت قبل از هر اقدام 1	FIA_UAU.2.1
43		سازوکار احرازهویت چندگانه 1	FIA_UAU.5.1
44		سازوکار احرازهویت چندگانه 2	FIA_UAU.5.2
45		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر 1	FIA_USB.1.1
46		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر 2	FIA_USB.1.2
47		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر 3	FIA_USB.1.3
48		الزامات پروتکل X509 (1)	FIA_X509_EXT.1.1/Rev
49		الزامات پروتکل X509 (2)	FIA_X509_EXT.1.2/Rev
50		الزامات پروتکل X509 (3)	FIA_X509_EXT.2.1
51	مدیریت امنیت	مدیریت کارکرد در محصول 1	FMT_MOF.1.1
52		مدیریت مشخصه های امنیتی 1	FMT_MSA.1.1
53		مدیریت مشخصه های امنیتی 3	FMT_MSA.3.1
54		مدیریت مشخصه های امنیتی4	FMT_MSA.3.2
55		مدیریت داده‌های محصول 1 – مدیر سیستم	FMT_MTD.1.1(1)
56		مدیریت داده‌های محصول 1 – کاربر عادی، وارد کننده داده	FMT_MTD.1.1(2)
57		کارکردهای مدیریتی محصول 1	FMT_SMF.1.1
58		نقش‌های امنیتی 1	FMT_SMR.1.1
59		نقش‌های امنیتی 2	FMT_SMR.1.2
60	حفاظت از توابع امنیتی محصول	حفظ وضعیت امن در زمان شکست 1	FPT_FLS.1.1
61		انتقال داده امنیتی در داخل محصول 1	FPT_ITT.1.1
62		سازگاری داده امنیتی بین محصول و موجودیت امن 1	FPT_TDC.1.1

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
63		**سازگاری داده امنیتی بین محصول و موجودیت امن 2**	FPT_TDC.1.2
64		**مهرهای زمانی 1**	FPT_STM.1.1
65		**به‌روز رسانی امن 2**	FPT_TUD_EXT.1.2
66		**به‌روز رسانی امن 3**	FPT_TUD_EXT.1.3
67	**تخصیص منابع**	**تحمل خطا 1**	FRU_FLT.1.1
68	**دسترسی به محصول**	**سوابق دسترسی به محصول 1**	FTA_TAH.1.1
69		**سوابق دسترسی به محصول 2**	FTA_TAH.1.2
70		**سوابق دسترسی به محصول 3**	FTA_TAH.1.3
71		**برقراری نشست 1**	FTA_TSE.1.1
72		**محدودیت بر روی چندین نشست همزمان 1**	FTA_MCS.1.1
73		**محدودیت بر روی چندین نشست همزمان 2**	FTA_MCS.1.2
74		**خاتمه دادن به نشست ها توسط محصول 1**	FTA_SSL.3.1
75		**خاتمه دادن به نشست ها توسط کاربر 1**	FTA_SSL.4.1
76		**مسیر امن 1**	FTP_TRP.1.1
77		**مسیر امن 2**	FTP_TRP.1.2
78		**مسیر امن 3**	FTP_TRP.1.3
79	**کانال‌های/مسیرهای مورد اعتماد**	**کانال امن 1**	FTP_ITC.1.1
80		**کانال امن 2**	FTP_ITC.1.2
81		**کانال امن 3**	FTP_ITC.1.3
82		**الزامات پروتکل X509**	FIA_X509_EXT.2.2

5-1-1- کلاس ممیزی امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_GEN.1	-	1	**FAU_GEN.1.1**	محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید: • آغاز و اتمام توابع ممیزی؛ • تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در کلاس ممیزی امنیت آمده است.
		2	**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 • **[آدرس IP ، شناسه کاربر، نوع فعالیت، تاریخ، زمان]**
FAU_GEN.2	- FAU_GEN.1	3	**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_SAR.1	4	**FAU_SAR.1,1**	محصول باید امکان خواندن [**شناسه کاربر، تاریخ، زمان، آدرس IP**] از کل رکوردهای ممیزی را برای [**مدیر سیستم**] فراهم نماید.
		5	**FAU_SAR.1,2**	محصول باید رکوردهای ممیزی را طوری فراهم نماید که کاربر بتولند آن‌ها را درک و اطلاعات این رکوردها را تفسیر نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_SAR.2	- FAU_SAR.1	6	**FAU_SAR.2.1**	محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.
FAU_SAR.3	- FAU_SAR.1	7	**FAU_SAR.3.1**	محصول باید امکان انجام **[جستجو، مرتب‌سازی]** رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس **[حساب کاربری، تاریخ/زمان، مکان، روش اتصال کاربر، درجه اهمیت رکوردها، نوع رخداد ، آدرس آی پی]** مرتب نماید.
FAU_STG.1	-	8	**FAU_STG.1.1**	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید.
FAU_STG.1	-	9	**FAU_STG.1.2**	محصول باید قادر به [تشخیص، جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد.
FAU_STG.3	-	10	**FAU_STG.3.1**	محصول در صورت تجاوز دنباله ممیزی از **[یک محدودیت از پیش تعریف شده]** باید با استفاده از **[یک کلنال ارتباطی، پیام کوتاه‌یا معادل آن، از طریق واسطهای محصول کاربران مربوطه را]** مطلع نماید.
FAU_STG.4	-	11	**FAU_STG.4.1**	محصول در صورت پر شدن دنباله ممیزی، باید [رویدادهای ممیزی را نادیده بگیرد،] و **[هیچ معیار انتخاب دیگری]**.
FAU_SEL.1	-	12	**FAU_SEL.1.1**	محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید: • [هویت موجودیت فعال، نوع رخداد] • **[هیچ معیار انتخاب دیگری]**

لیست رویدادهای قابل ممیزی

مولفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد 1	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی 1	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی 1	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی‌که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
اقدامات لازم در زمان از دست رفتن داده ممیزی 1	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی 1	عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
صحت داده های کاربری ذخیره شده 2	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
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 سازو کار احرازهویت فعال همراه با نتیجه نهائی (پایه)	
شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال

مدیریت کلمه عبور	ثبت رد هر کلمه عبور تست شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
مدیریت مشخصه‌های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	
مدیریت داده های محصول 1-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
مدیریت داده های محصول 1-کاربرعادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
عملیات رمزنگاری 1(1)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
عملیات رمزنگاری 1 (2)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
عملیات کنترل دسترسی 1	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل)	شناسایی داده‌های موجودیت غیرفعال

	تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	
ورود داده‌های کاربری به محصول با مشخصه امنیتی	ورود داده کاربری موفقیت آمیز، شامل هر گونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	
خروج داده های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	
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 می‌باشد (حداقل)	
سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	
حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)	
تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست می‌باشد (پایه)	
برقراری نشست 1	ثبت منع آغاز نشست بدلیل مکانیزم 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)	
خاتمه دادن به نشست ها	ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	

2-1-5- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.1	FCS_COP.1.1(1) -	13	**FCS_COP.1.1(1)**	محصول باید [**برای وارسی صحت داده‌های ممیزی و داده‌های رکورد**] بر اساس یک الگوریتم رمزنگاری مشخص [**AES**] و اندازه کلید رمزنگاری [**256**] اجرا شود که مطابق با [RSA] باشد. داده های ممیزی بدون مکانیزم خاصی ذخیره شده و به منظور حفظ امنیت، فقط مدیر قادر به مشاهده آن میباشد.
		14	**FCS_COP.1.1(2)**	محصول باید [**برای تولید داده درهم‌سازی**] بر اساس مجموعه الگوریتم‌های رمزنگاری مشخص[**BCRYPT-SHA384**] و اندازه‌کلید رمزنگاری [**هیچ**] اجرا شود که مطابق با [**RSA**]باشد.
FCS_HTTPS_EXT.1	-	15	**FCS_HTTPS_EXT.1.1**	محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.
		16	**FCS_HTTPS_EXT.1.2**	محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.
		17	**FCS_HTTPS_EXT.1.3**	درصورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [اتصال را برقرار ننماید ، هیچ اقدام دیگری انجام ندهد].
FCS_TLSC_EXT.1	-	81	**FCS_TLSC_EXT.1.1**	محصول باید [TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:] o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 o TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246 o TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				o TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256 مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246 o TLS _RSA_WITH_AES_128_GCM_ SHA256 مطابق با RFC 5288 o TLS _RSA_WITH_AES_192_GCM_ SHA256 مطابق با RFC 5288 o TLS _RSA_WITH_AES_256_GCM_ SHA384 مطابق با RFC 5288 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق باRFC 5289 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289].
		19	**FCS_TLSC_EXT.1.2**	محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید نماید.
		20	**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، برای برقراری ارتباط درخواست مجوز بدهد، [**هیچ اقدام دیگری**]].
		21	**FCS_TLSC_EXT.1.4**	محصول باید [Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [secp384r1, secp521r1]][و **هیچ منحنی دیگری**] در پیام ClientHello ارائه دهد.
FCS_TLSS_ EXT.1	-	22	**FCS_TLSS_EXT.1.1**	محصول باید [TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 هیچ مجموعه رمز دیگری]].
		23	**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.
		24	**FCS_TLSS_EXT.1.3**	محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید 2048 بیت و [هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [secp256r1] و هیچ منحنی دیگری] ،[هیچ اندازه دیگری]] ایجاد نماید.
FCS_TLSS_EXT.2.	-	25	**FCS_TLSS_EXT.2.4**	محصول باید احرازهویت دوطرفه کلاینت‌های TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.
		26	**FCS_TLSS_EXT.2.5**	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، برای برقراری ارتباط درخواست مجوز بدهد، [**هیچ اقدام دیگری**]].

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		27	**FCS_TLSS_EXT.2.6**	محصول در صورت مطابقت نداشتن؛ نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه که از شناساننده[1] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد.

[1] Identifier

3-1-5- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ **[هیچ عملیات دیگری]**]
FDP_ACF.1	- FDP_ACF.1,1	32	**FDP_ACF.1,1**	محصـــول باید [**خط‌مشـــی‌های کنترل دســـترســـی]** را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید:

[2] Metadata

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				] • **هویت کاربر** • **نقش‌ها و مجوزهای کاربر مجاز**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				• **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می-شوند** • **[هیچ مشخصه دیگری]**]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
		33	**FDP_ACF.1,2**	محصـــول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				[**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.**]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
		34	**FDP_ACF.1,3**	محصول باید براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد:]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				• **کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند.**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				• **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
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
		35	**FDP_ACF.1.4**	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید:]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
				• **تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[۳] از پیش تعریف شده،**

[3] Threshold

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ **[هیچ عملیات دیگری]**]
				• [**هیچ قانون دیگری**]]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
FDP_RIP.2	-	36	**FDP_RIP.2.1**	محصول باید تضمین نماید در هنگام [تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
FDP_SDI.2	-	37	**FDP_SDI.2.1**	محصـــول باید داده کاربری حســـاس و یا دارای بار حقوقی ذخیره شـــده در مکان تحت کنترل خود را برای تشـــخیص [**خطاهای صـــحت داده**] داده های رکورد و داده¬های ممیزی را بر اساس مشخصه های [**درهم شده داده های کاربری ذخیره شده**] پایش نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.1		31	**FDP_ACC.1.1**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید:] • موجودیت فعال: [**مدیر سیستم، کاربر عادی، کاربر مهمان، مدیر ارشد**] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[۲] ○ داده متعلق به کاربران ○ داده احرازهویت ○ داده با این معیارها: [**داده های دارای سطح دسترسی**] ○ [**هیچ موجودیت دیگری**] • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی‌ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال ○ [**هیچ عملیات دیگری**]]
		38	**FDP_SDI.2.2**	هنگام تشخیص خطای صحت داده، محصول باید [**اقدام لازم**] را صورت دهد.

4-1-5- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_UID.1	-	28	**FIA_UID.1.1**	محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد: [• **مشاوره راهنمای نحوه ورود به سیستم،** • **[هیچ اقدام دیگر]**]
		29	**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_AFL.1	- FIA_AFL.1.1	30	**FIA_AFL.1.1**	محصول باید بتواند وقوع یک عدد مثبت قابل تنظیم توسط مدیر در بازه‌ی **[6,5]** تلاش ناموفق احرازهویت مرتبط با [**احراز هویت کاربر در هنگام ورود به سامانه و یا اعتبارسنجی پسورد**]را تشخیص دهد.
		39	**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 [**لیستی از اقدامات مقابله‌ای**] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.
FIA_ATD.1	-	40	**FIA_ATD.1.1**	محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				] • **شناسه کاربر** • **متد احرازهویت مورد استفاده** • **داده احرازهویت** • **نقش کاربر** • **وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)** • **[هیچ مشخصه امنیتی دیگر]** [
FIA_PMG_EXT.1	-	41	**FIA_PMG_EXT.1.1**	محصـــول باید قابلیت‌های مدیریت کلمه عبور را که در زیر ذکر شـــده‌اند برای کلمه‌های عبور مدیریتی فراهم نماید: 1. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [*"@"، "#"، "$"، "٪"، "^"، "/"، "&"، "*"، ")" , "("*]**هیچ کاراکتر دیگر**]] باشد. 2. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و 15 کاراکتر یا بیشتر باشد.
FIA_UAU.2	-	42	**FIA_UAU.2.1**	محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت نماید.
FIA_UAU.5	-	43	**FIA_UAU.5.1**	محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد: **[احراز هویت از طریق پیام کوتاه]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_UAU.5	-	44	**FIA_UAU.5.2**	محصول باید هر کاربر متقاضی احراز هویت را مطابق با قوانین ذیل احراز هویت نماید.:] • **کاربران راه دور علاوه بر نام کاربری و کلمه عبور بر اساس احراز هویت چندگانه (مانند Dual factor authentication) استفاده نمایند.** • **احرازهویت مبتنی بر توکن و از این قبیل موارد** [
FIA_USB.1	-	45	**FIA_USB.1.1**	محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:] • **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق)** • **[هیچ مشخصه دیگری]** [
		46	**FIA_USB.1.2**	محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:] • **زمانی‌که یک نشست جدید برقرار می‌شود، اعتبار نشست‌های قبلی باید از بین برود (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد و هنگام فعال شدن نشست دوم و بیشتر در برنامه، باید به صفحه کاربر نشست اصلی(اول) اطلاع داده شود.)**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **اطلاعات پیشینه احراز هویت باید بروزرسانی گردد** • [**هیچ قانون دیگری**]]
		47	**FIA_USB.1.3**	محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: [• **هیچ تغییری در طول نشست فعال مجاز نمی‌باشد،** • **[هیچ قانون دیگری]**]
FIA_X509_EXT.1	-	48	**FIA_X509_EXT.1.1/Rev**	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای [**TLS, HTTPS**]، و [امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم، امضای کد برای تأیید یکپارچگی، [**سایر کاربردها**]، **هیچ کاربرد دیگر**] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.
		49	**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.

5-1-5- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.1	-	50	**FMT_MOF.1.1**	محصـــول 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 و [هیچ نقش دیگری]]** محدود نماید.
FMT_MSA.1	-	51	**FMT_MSA.1.1**	• محصول باید با اعمال [**خط‌مشی کنترل دسترسی**]، امکان تغییر پیش‌فرض، [پرس و جو، تغییر، حذف، [**هیچ عملیات دیگری**]] مشخصه‌های امنیتی [**شناسه کاربر، نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه، جزئیات واسط کلاینت، پیشینه احراز هویت**] را به [**مدیر سیستم و هر کاربری که مجوز لازم را دارد**] محدود نماید.
FMT_MSA.3	-	52	**FMT_MSA.3.1**	محصول برای مشخصه های امنیتی که برای اعمال [**خط مشی**] استفاده می شوند، باید مقادیر پیش فرض محدود شده ای درنظر بگیرد.
		53	**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	-	54	**FMT_MTD.1.1(1)**	محصـــول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن ، [**هیچ کارکرد دیگر**]] [**داده‌های ممیزی و داده‌های احراز هویت**] به [**مدیر سـیسـتم** [**هیچ نقش دیگری**]] محدود نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		55	**FMT_MTD.1.1(2)**	محصـــول باید توانایی [تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [**هیچ کارکرد دیگر**]] [**داده‌های تحت مالکیت کاربر عادی**] به [**کاربر عادی**] محدود نماید.
FMT_SMF.1	-	56	**FMT_SMF.1.1**	محصـــول باید قادر به انجام [**کارکردهای مدیریتی که در جدول زیر آمده اســت**] باشد:

مولفه	عملیات مدیریتی
بازبینی داده ممیزی 1	پشـتیبانی از (حذف، ویرایش، اضـافه) گروهی از کاربران با مجوز دسـترسـی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی 1	پشـتیبانی از مجوزهای مشـاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دسـت رفتن داده ممیزی 1	پشـتیبانی از حد آسـتانه و از عملیات (حذف، ویرایش، اضـافه) در زمان خرابی ذخیره‌سـازی ممیزی
پیشـگیری از اتلاف و از بین رفتن داده‌های ممیزی 1	پشـتیبانی از عملیات (حذف، ویرایش، اضـافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشـخصـه‌های مورد اسـتفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده در منابع	انتخـاب هنگـام اجرای حفـاظـت از اطلاعـات باقی‌مانده (برای مثال، تخصـیص و یا آزاد

مؤلفه	وابستگی ها	شماره	المان	شرح المان	
					سازی) که می‌تواند در محصول قابل پیکربندی باشد.
				ورود داده های کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
				صحت داده های کاربری ذخیره شده 2	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
				مدیریت احراز هویت ناموفق	مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
				تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد. [اختیاری]
				مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت‌ها برای تنظیم کلمه عبورها
				احراز هویت کاربر	مدیریت داده‌های احرازهویت 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]اختیاری[مدیریت تغییرات و فرایندهایی مانند(اختصاص ادرس IP برای عملیات

مؤلفه	وابستگی ها	شماره	المان	شرح المان	
					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 مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و تغییر دهد.
				مدیریت مشخصه‌های امنیتی	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
				مقدار دهی اولیه مشخصه‌ها	مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
				مدیریت داده های محصول 1-مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
				مدیریت داده های محصول 1-کاربرعادی، وارد کننده داده	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
				نقش‌های امنیتی	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
				محدودیت بر روی چندین نشست همزمان	مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر
				برقراری نشست	مدیریت شرایط آغاز نشست توسط مدیر مجاز

مؤلفه	وابستگی ها	شماره	المان	شرح المان	
				خاتمه دادن به نشست ها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.
FMT_SMR.1	- FMT_SMR.1.1	57	**FMT_SMR.1.1**	نقش‌های زیر در محصول باید تعریف شده باشد: [مدیر سیستم، کاربر عادی، [**سایر نقش‌های قابل تعریف در سیستم**]]]]	
		58	**FMT_SMR.1.2**	محصول، باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند.	

6-1-5- کلاس حفاظت از توابع امنیتی هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.1	-	59	**FPT_FLS.1.1**	محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [**شکست‌های نرم‌افزاری، شکست‌های کاربری**]
FPT_ITT.1	- FTP_TRP.1.1	60	**FPT_ITT.1.1**	محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که باهم ارتباط دارند، محافظت نماید.
FPT_TDC.1	- FTP_TRP.1.1	61	**FPT_TDC.1.1**	محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [**داده‌های ممیزی و داده‌های احراز هویت**] را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد
		62	**FPT_TDC.1.2**	محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [**لیستی از قوانین تفسیر که در محصول به کار می‌روند**] استفاده نماید.
FPT_STM.1	-	63	**FPT_STM.1.1**	محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و مکانیزم کارکردی صحیح برطرف نماید.
FPT_TUD_EXT.1	-	64	**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 به‌روزرسانی‌های خودکار پشتیبانی کند].
		65	**FPT_TUD_EXT.1.3**	محصول مورد ارزیابی باید در صورت استفاده از به روز رسانی به روش خودکار، پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [مکانیسم امضای دیجیتال،

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.

7-1-5- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.1	-	66	**FRU_FLT.1.1**	محصول باید از عملکرد [**تمام کارکردهای اصلی**] هنگام رویداد شکست‌های زیر اطمینان حاصل نماید: **[شکست نرم‌افزاری[هیچ شکست دیگری]]**

8-1-5- کلاس دسترسی به هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_TAH.1	-	67	FTA_TAH.1.1	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست براساس [روز، زمان، [**هیچ مشخصه دیگری**]] باشد.
		68	FTA_TAH.1.2	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید [تاریخ، زمان، متد، مکان] آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.
		69	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	-	70	FTA_TSE.1.1	توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس [**مکان ، تعداد تلاش های ناموفق احرازهویت، شناسه کاربر(نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP** [دیگر **هیچ مشخصه دیگر**]] ممانعت نماید.
FTA_MCS.1	- FTA_MCS.1.1	71	FTA_MCS.1.1	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید
		72	FTA_MCS.1.2	محصول باید به صورت پیش‌فرض، [**تعداد نشست همزمان پیش‌فرض**] برای هر کاربر در نظر بگیرد.
FTA_SSL.3	- FTA_MCS.1.1	73	FTA_SSL.3.1	محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمان [**بازه زمانی که توسط مدیرتنظیم می‌شود**] غیرفعال بودن، خاتمه دهد
FTA_SSL.4	- FTA_MCS.1.1	74	FTA_SSL.4.1	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.1	-	75	**FTP_TRP.1.1**	محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [**TLS, HTTPS**] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کلنال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال¬ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده¬های تبادلی حفاظت نماید و تغییرات را تشخیص دهد.
		76	**FTP_TRP.1.2**	محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.
		77	**FTP_TRP.1.3**	محصول مورد ارزیابی باید استفاده از کانال امن را برای احرازهویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی نماید.

9-1-5- کلاس کانال‌ها و مسیرهای مورد اعتماد

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_ITC.1	-	78	**FTP_ITC.1.1**	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [SSH, TLS, HTTPS] میان خود و موجودیت IT معتبر، سرور ممیزی، [سرور احرازهویت، **هیچ قابلیت 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.
		79	**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.
		80	**FTP_ITC.1.3**	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [**خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند**] راه‌اندازی نماید
FIA_X509_EXT.2	-	81	**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 [به مدیر سیستم این امکان را بدهد که در زمینه‌ی پذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد.]

توجیهات:

- به دلیل عدم پشتیبانی امضا دیجیتال در سیستم، الزامات FDP_ITC.2 و FDP_ETC.2 اتفاق نمی‌افتد

2-5- الزامات تضمین امنیتی

اهداف امنیتی تعریف شده در بخش 5 جهت مقابله نمودن با تهدیدات معرفی شده در بخش 4 در نظر گرفته شده‌اند. الزامات کارکردی در بخش 6 بیان رسمی و استانداردی از «اهداف امنیتی» می‌باشد. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا براساس این الزامات ارزیابی، مستندات را ارزیابی و تست مستقل برروی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به صورت زیر می‌باشد:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول رادر اختیار آزمایشگاه قرار می‌دهد و محیط تست آن را فراهم می‌نماید. و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Life cycle Support	ALC_CMC.1	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول
Security Target	ASE_CCL.1	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.1	اهداف امنیتی
	ASE_REQ.1	الزامات امنیتی معین
	ASE_TSS.1	خلاصه مشخصات هدف ارزیابی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری

کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی‌باشد، اما در صورت وجود باید محتوای آن با الزمات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسط‌های کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسط‌ها نمی‌باشد. فعالیت‌های این خانواده باید بر روی شناخت واسط‌های معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی1** **شماره مولفه: (ADV_FSP.1.1D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی1 **شماره مولفه: (ADV_FSP.1.2D)** **شرح مولفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی1** **شماره مولفه: (ADV_FSP.1.1C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [4]و پشتیبان کننده‌ی الزام کارکرد امنیتی[5]توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی1 **شماره مولفه: (ADV_FSP.1.2C)**

[4]-SFR-enforcing TSFI
[5]-SFR-supporting TSFI

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی1 **شماره مولفه: (ADV_FSP.1.3C)** **شرح مولفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی1 **شماره مولفه: (ADV_FSP.1.4C)** **شرح مولفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی1** **شماره مولفه: (ADV_FSP.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی1 **شماره مولفه: (ADV_FSP.1.2E)** **شرح مولفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «تست» و «آسیب‌پذیری» ارائه شده است.

کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر

دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

راهنمای کاربردی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی 1** **شماره مولفه: (AGD_OPE.1.1D)** **شرح مولفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی 1** **شماره مولفه: (AGD_OPE.1.1C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی 1 **شماره مولفه: (AGD_OPE.1.2C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی 1

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مولفه: (AGD_OPE.1.3C) **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی 1 **شماره مولفه: (AGD_OPE.1.4C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی 1 **شماره مولفه: (AGD_OPE.1.5C)** **شرح مولفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی 1 **شماره مولفه: (AGD_OPE.1.6C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی 1 **شماره مولفه: (AGD_OPE.1.7C)** **شرح مولفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی 1** **شماره مولفه: (AGD_OPE.1.1E)**

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مولفه‌های محتوایی را برآورده می‌نماید.

راهنمای آماده‌سازی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی 1** **شماره مولفه: (AGD_PRE.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی 1** **شماره مولفه: (AGD_PRE.1.1C)** **شرح مولفه:** مستندات آماده‌سازی بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی 1 **شماره مولفه: (AGD_PRE.1.2C)** **شرح مولفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مولفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی 1** **شماره مولفه: (AGD_PRE.1.1E)** **شرح مولفه:**

مولفه‌های اقدامات ارزیاب	
	ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی 1 **شماره مولفه: (AGD_PRE.1.2E)** **شرح مولفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.

کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان(EAL1) تنها به این اطلاعات نیاز است.

قابلیت‌های پیکربندی

این مولفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول 1** **شماره مولفه: (ALC_CMC.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول 1** **شماره مولفه: (ALC_CMC.1.1C)**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول 1** **شماره مولفه: (ALC_CMC.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

حوزه پیکربندی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول 1** **شماره مولفه: (ALC_CMS.1.1D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول 1** **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول 1 **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول 1** **شماره مولفه: (ALC_CMS.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

کلاس هدف امنیتی

ارزیابی سند هدف امنیتی برای اطمینان از شفاف بودن و نداشتن ناسازگاری داخلی لازم است. همچنین اگر سند هدف امنیتی از یک یا چند پروفایل حفاظتی استفاده کرده است، تضمین درست بودن آن و انتخاب‌های درست صورت گرفته شده در آن، لازم است.

ادعاهای انطباق

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق 1** **شماره مولفه: (ASE_CCL.1.1D)** **شرح مولفه:** توسعه دهنده باید یک ادعای انطباق تهیه نماید.
	نام عنصر: ادعاهای انطباق 1 **شماره مولفه: (ASE_CCL.1.2D)** **شرح مولفه:** توسعه دهنده باید ارتباط منطقی ادعای انطباق تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق 1** **شماره مولفه: (ASE_CCL.1.1C)** **شرح مولفه:** ادعای انطباق باید حاوی یک ادعای انطباق معیار مشترک باشد، که نسخه‌ی معیار مشترک که سند هدف امنیتی و محصول ادعای انطباق با آن دارند را مشخص نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: ادعاهای انطباق 1 **شماره مولفه: (ASE_CCL.1.2C)** **شرح مولفه:** ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش 2 انطباق یا توسعه معیار مشترک را توصیف نماید.
	نام عنصر: ادعاهای انطباق 1 **شماره مولفه: (ASE_CCL.1.3C)** **شرح مولفه:** ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش 3 انطباق یا توسعه معیار مشترک را توصیف نماید.
	نام عنصر: ادعاهای انطباق 1 **شماره مولفه: (ASE_CCL.1.4C)** **شرح مولفه:** ادعای انطباق معیار مشترک باید با تعریف مؤلفه‌های توسعه‌یافته سازگار باشد.
	نام عنصر: ادعاهای انطباق 1 **شماره مولفه: (ASE_CCL.1.5C)** **شرح مولفه:** ادعای انطباق معیار مشترک باید تمامی پروفایل‌های حفاظتی و بسته‌های الزامات امنیتی که ادعاهای انطباق سند هدف امنیتی آن‌ها را بیان دارد، را شناسایی کند.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق 1** **شماره مولفه: (ASE_CCL.1.1E)** **شرح مولفه:** ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

تعریف مؤلفه‌های توسعه‌یافته

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1** **شماره مولفه: (ASE_ECD.1.1D)** **شرح مولفه:** توسعه دهنده باید یک اظهارنامه از الزامات امنیتی تهیه نماید.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.2D)** **شرح مولفه:** توسعه دهنده باید یک تعریف مؤلفه‌های توسعه‌یافته تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1** **شماره مولفه: (ASE_ECD.1.1C)** **شرح مولفه:** اظهارنامه الزامات امنیتی باید تمامی الزامات امنیتی توسعه‌یافته را مشخص نماید.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.2C)** **شرح مولفه:** تعریف مؤلفه‌های توسعه‌یافته باید یک مؤلفه توسعه‌یافته برای هر الزام امنیتی توسعه‌یافته تعریف نماید.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.3C)** **شرح مولفه:** تعریف مؤلفه‌های توسعه‌یافته باید توصیف کند که چگونه هر مؤلفه توسعه‌یافته به مؤلفه‌های معیار مشترک، خانوادها و کلاس‌ها مرتبط می‌شود.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.4C)** **شرح مولفه:**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	تعریف مؤلفه‌های توسعه‌یافته باید از مؤلفه‌های معیار مشترک موجود، خانوادها، کلاس‌ها و متدولوژی به عنوان یک مدل برای ارائه، استفاده نماید.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.5C)** **شرح مولفه:** مؤلفه‌های توسعه‌یافته باید شامل إلمان‌های هدفمند و قابل‌اندازه گیری باشد، طوری که انطباق و عدم انطباق با این إلمان‌ها، قابل اثبات باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1** **شماره مولفه: (ASE_ECD.1.1E)** **شرح مولفه:** ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته1 **شماره مولفه: (ASE_ECD.1.2E)** **شرح مولفه:** ارزیاب باید تایید نماید که هیچ مؤلفه‌ی توسعه‌یافته‌ای به وسیله مؤلفه‌های موجود، به صورت شفاش قابل بیان نمی‌باشد.

معرفی هدف امنیتی

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی **(ASE_INT)**	**نام عنصر: معرفی هدف امنیتی 1** **شماره مولفه: (ASE_INT.1.1D)** **شرح مولفه:** توسعه دهنده باید یک سند معرفی هدف امنیتی تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی **(ASE_INT)**	**نام عنصر: معرفی هدف امنیتی 1** **شماره مولفه: (ASE_INT.1.1C)** **شرح مولفه:** سند معرفی هدف امنیتی باید شامل مرجع هدف امنیتی، مرجع محصول، توصیف محصول و مرور کلی محصول باشد.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.2C)** **شرح مولفه:** مرجع سند هدف امنیتی باید هدف امنیت را به‌صورت منحصربه‌فرد مشخص نماید.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.3C)** **شرح مولفه:** مرجع محصول باید محصول را مشخص نماید.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.4C)** **شرح مولفه:** مرور کلی محصول باید نحوه استفاده و ویژگی‌های اصلی محصول را به صورت خلاصه بیان نماید.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.5C)** **شرح مولفه:** مرورکلی محصول باید نوع محصول را معرفی نماید.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.6C)** **شرح مولفه:** مرور کلی محصول باید هر سخت‌افزار/نرم‌افزار/ثابت‌افزار غیر از محصول مورد ارزیابی، که بوسیله محصول استفاده می‌شود را معرفی نماید.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.7C)** **شرح مولفه:** شرح محصول باید حوزه فیزیکی محصول را توصیف نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.8C)** **شرح مولفه:** شرح محصول باید حوزه منطقی محصول را توصیف نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی **(ASE_INT)**	**نام عنصر: معرفی هدف امنیتی 1** **شماره مولفه: (ASE_INT.1.1E)** **شرح مولفه:** ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: معرفی هدف امنیتی 1 **شماره مولفه: (ASE_INT.1.2E)** **شرح مولفه:** ارزیاب باید تایید نماید که مرور کلی محصول، مرجع محصول و خلاصه محصول با یکدیگر سازگار هستند.

اهداف امنیتی

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی 1** **شماره مولفه: (ASE_OBJ.1.1D)** **شرح مولفه:** توسعه‌دهنده باید که اظهارنامه از اهداف امنیتی تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی 1**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مولفه: (ASE_OBJ.1.1C) **شرح مولفه:** اظهارنامه اهداف امنیتی باید اهداف امنیتی برای محیط عملیاتی را توصیف نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی 1** **شماره مولفه: (ASE_OBJ.1.1E)** **شرح مولفه:** ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

الزامات امنیتی معین

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین 1** **شماره مولفه: (ASE_REQ.1.1D)** **شرح مولفه:** توسعه‌دهنده باید که اظهارنامه از اهداف امنیتی تهیه نماید.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.2D)** **شرح مولفه:** توسعه‌دهنده باید ارتباط منطقی بین الزامات را تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین 1** **شماره مولفه: (ASE_REQ.1.1C)**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: اظهارنامه الزامات امنیتی باید الزامات کارکردی و تضمین امنیت راتوصیف نماید.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.2C)** **شرح مولفه:** تمامی موجودیت‌های فعال، غیرفعال، عملیات، مشـــخصـــه‌های امنیتی، موجودیت‌های خارجی و دیگر اصـــطلاحاتی که در الزامات کارکردی و تضمین امنیت استفاده می‌شوند، باید توصیف گردند.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.3C)** **شرح مولفه:** اظهارنامه الزامات امنیتی باید تمامی عملیات بر روی الزامات امنیتی را معرفی نماید.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.4C)** **شرح مولفه:** تمامی عملیات باید به درستی انجام گیرند.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.5C)** **شرح مولفه:** هر وابستگی بین الزامات امنیتی باید ارضاء گردد، یا ارتباط منطقی الزامات امنیتی نشان دهد که نیاز به ارضاء نمی‌باشد.
	نام عنصر: الزامات امنیتی معین 1 **شماره مولفه: (ASE_REQ.1.6C)** **شرح مولفه:** اظهارنامه الزامات امنیتی باید سازگاری داخلی داشته باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین 1** **شماره مولفه: (ASE_REQ.1.1E)** **شرح مولفه:**

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

خلاصه مشخصات هدف ارزیابی

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی 1** **شماره مولفه: (ASE_TSS.1.1D)** **شرح مولفه:** توسعه‌دهنده باید یک سند خلاصه مشخصات محصول تهیه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی 1** **شماره مولفه: (ASE_TSS.1.1C)** **شرح مولفه:** سند خلاصه مشخصات محصول باید تشریح نماید که چگونه محصول الزامات کارکردی امنیت را برآورده می‌نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی 1** **شماره مولفه: (ASE_TSS.1.1E)** **شرح مولفه:** ارزیاب باید تایید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: خلاصه مشخصات هدف ارزیابی 1 **شماره مولفه: (ASE_TSS.1.1E)** **شرح مولفه:** ارزیاب باید تایید نماید که خلاصه مشخصات محصول با مرور کلی محصول و خلاصه محصول سازگار می‌باشد.

کلاس تست

تست محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آنها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. تست بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و تست بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) تست براساس کارکردی که برای محصول در نظر گرفته شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج تست و تحلیل آسیب‌پذیری باید در گزارش تست لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

تست مستقل

«تست مستقل» برای تائید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه شده، صورت می‌گیرند. هدف اصلی تست اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. ارزیاب باید در سند «گزارش تست»، طرح تست و نتایج آن را مستند نماید.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل 1** **شماره مولفه: (ATE_IND.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل 1** **شماره مولفه: (ATE_IND.1.1C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل 1** **شماره مولفه: (ATE_IND.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مولفه‌های محتوایی را برآورده می‌نماید.

مولفه‌های اقدامات ارزیاب	
	نام عنصر: تست مستقل 1 **شماره مولفه: (ATE_IND.1.2E)** **شرح مولفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

کلاس آسیب‌پذیری

این کلاس به پوشش آسیب‌پذیری‌های قابل بهره‌برداری که در توسعه و عملیات محصول ممکن وجود داشته باشد می‌پردازد.

تحلیل آسیب‌پذیری

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری 1** **شماره مولفه: (AVA_VAN.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارئه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری 1** **شماره مولفه: (AVA_VAN.1.1C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری 1** **شماره مولفه: (AVA_VAN.1.1E)**

مولفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
	شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری 1 **شماره مولفه: (AVA_VAN.1.2E)** **شرح مولفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری 1 **شماره مولفه: (AVA_VAN.1.3E)** **شرح مولفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

6- خلاصه مشخصات هدف ارزیابی

- **کلاس ممیزی امنیت**

اکثر عملیات انجام شده در سامانه ذخیره می‌گردد و در قسمت **عملکرد کاربران** قابل مشاهده می‌باشد. دقت داشته باشید که همه کاربران به این فرم دسترسی نداشته و فقط مدیران یا کاربرانی که به فرم **عملکرد کاربران** دسترسی دارند می‌توانند اطلاعات را مشاهده کنند. این اطلاعات شامل نام خانوادگی کاربر، نام کاربری، نوع رویداد، تاریخ ثبت، زمان ثبت، توضیحات ، IP و... می‌باشند که برای کاربر مشاهده کننده قابل درک و فهم می‌باشد. (FAU_GEN.1.1, FAU_GEN1.2, FAU_GEN2.1)

محصول قادر است تمامی رکوردهای ممیزی ثبت شده را به مدیر سیستم به صورت کاملا خوانا و قابل درک نمایش دهد و مدیر میتواند این اطلاعات را بر اساس نام کاربری و دیگر موارد مرتب نماید.(FAU_SAR.1.2, FAU_SAR1.1, FAU_SAR2.1, FAU_SAR.3.1)

مثال‌ها:

1. اگر کاربری به سامانه وارد شود، رکورد ممیزی در سامانه (فرم عملکرد کاربران) ذخیره می‌شود که در قسمت رویداد، مقدار "ورود به سامانه" ثبت می‌شود.

2. اگر کاربری برای ورود غیر مجاز تلاش کند(رمز اشتباه وارد کند) رکورد ممیزی ذخیره می‌گردد و در قسمت رویداد، وضعیت رویداد "ورود به سامانه"مقدار "ناموفق" ثبت می‌شود.
3. اگر پس از وارد کردن رمز اشتباه، حساب کاربری غیر فعال شود، در قسمت رویداد، مقدار "تلاش غیر مجاز برای ورود" ثبت میگردد.
4. اطلاعات ثبت شده در فرم رویدادها شامل نام‌خانوادگی کاربری که باعث ثبت رویداد شده است، نام کاربری(هویت کاربر)، نام رویداد، تاریخ و زمان ثبت رویداد، موقعیت یا IP، وضعیت رویداد رخ داده که میتواند موفق/ناموفق باشد. همچنین توضیحات و اطلاعات اضافه نیز میتواند در این فرم ذخیره شود. این اطلاعات فقط برای کاربر مدیر یا هر کاربری که نقش مدیر را داشته باشد نمایش داده میشود.
5. در فرم عملکرد کاربران، مدیر میتواند اطلاعات را بر اساس ستون‌های موجود، مرتب کند(با کلیک روی هر ستون). همچنین مدیر میتولند بر اساس تاریخ، نوع رویداد، نام‌خانوادگی، نام کاربری و IP ،اطلاعات را جستجو کند.
6. بخاطر اینکه اطلاعات موجود در عملکرد کاربران امنیتی میباشد، قابلیت حذف آن‌ها وجود ندارد و تمامی رویدادها برای مدیر قابل نمایش و قابل فهم میباشد.
7. صحت اطلاعات رویدادها در فرم عملکرد کاربران چک میشود. اگر اطلاعاتی از جدول مربوطه(user_event) تغییر کند، در فرم عملکرد کاربران، رکورد تغییر یافته به صورت قرمز رنگ نمایش داده میشود که مدیر متوجه این تغییر شود. در صورتی که اطلاعات ممیزی از طریق دیتابیس توسط کاربر تغییر کند، لاگی با عنوان دستکاری غیر مجاز ثبت میشود. این موارد مربوط به الزامات FAU_STG.1.1 و FAU_STG.1.2 میباشد.
8. در صورتی که اطلاعات ممیزی از حد آستانه عبور کند، پیامی به مدیر سامانه به منظور اطلاع رسانی از این مورد ارسال میشود. حد آستانه توسط مدیر در فرم پیکربندی لاگ‌ها قابل تغییر است. همچنین لاگی با عنوان پیامک هشدار نیز در فرم عملکرد کاربران ذخیره میشود. الزام FAU_STG.3.1 .
9. پس از ارسال پیام به مدیر سامانه به منظور اطلاع رسانی از عبور از حد آستانه، مدیر 24 ساعت(این زمان در فرم پیکربندی لاگ قابل تغییر است) وقت دارد که از داده‌های قبلی در صورت نیاز فایل پشتیبان تهیه کند(چاپ) در غیر اینصورت پس از 24 ساعت، رکوردهای ممیزی حذف خواهند شد. الزام FAU_STG.4.1
10. مدیر میتواند در فرم فعال سازی لاگ‌ها، رویدادهایی که میخواهد در سیستم ثبت شود را فعال/غیرفعال کند. در صورتی که رویداد مربوطه غیر فعال باشد، در نتیجه لاگی هم ثبت نمیشود. الزام FAU_SEL.1.1

- **پشتیبانی از رمزنگاری**

محصول میتواند رمز عبور تعریف شده توسط کاربر را توسط الگوریتم BCRYPT-SHA384 رمز و درهم سازی کند که این امر باعث میشود رمز ذخیره شده از امنیت بالایی برخوردار شود. مقادیر ابتدا به base64تبدیل و سپس به BCRYPT-SHA384 تبدیل میشوند

برای ارتباط با سایر قسمتها، محصول ارتباط امن مبنی بر پروتکل https و tls برقرار میکند (FCS_TLSS.1.1و FCS_TLSS.1.2 و FCS_TLSS.1.3)

همچنین محصول میتواند هنگام ارتباط با سرویس ارسال sms ، ارتباط امن را برقرار نماید و از صحت اطلاعات اطمینان حاصل کند(FCS_TLSC_EXT.1.1, FCS_TLSC.1.3, FCS_TLSC_EXT.1.3, FCS_TLSC_EXT.1.2)

مثال‌ها:

1. در جدول مربوط به ثبت داده ممیزی(user_event)، فیلدی به نام hash اضافه گردید که مقدار آن برابر است با اطلاعات همان رکورد به صورت رمز شده(AES). با استفاده از این فیلد، سامانه صحت اطلاعات ممیزی را بررسی میکند.
2. رمز عبور تعریف شده توسط کاربران، از الگوریتم BCRYPT-SHA384 برای درهم سازی استفاده میکند. این الگوریتم به دلیل امنیت بالایی که دارد در سامانه استفاده شده است.
3. محصول برای برقراری ارتیاط با اجزاء خارجی، از کانال امن(TLS) استفاده میکند که باعث میشود اطلاعات ارسال شده به خارج از سامانه به صورت امن انجام شود و از فیشینگ اطلاعات جلوگیری شود.
4. تمامی cipher suite های بیان شده در ارتباط با دیتابیس و ارسال SMS لحاظ شده است.

- **حفاظت از داده کاربری**

مدیریت سطح دسترسی سامانه بر اساس سیستم مدیریت نقش کاربران(RBAC) می‌باشد. یعنی مدیر ارشد می‌تواند نقش‌های مورد نیاز را ایجاد و به کاربران انتصاب دهد. تمامی اطلاعات و فرم‌های موجود در سامانه دارای سطح دسترسی می‌باشند و هر کاربر فقط به قسمت‌هایی که مدیر ارشد تعیین کرده دسترسی دارد و می‌تواند اطلاعات را مشاهده، ویرایش و ذخیره نماید. سامانه به داده‌های غیر مجاز حساس بوده و هنگام ورود اطلاعات در فرم‌ها توسط کاربر ، داده‌های غیر مجاز شناسایی و از ذخیره شدن آن‌ها جلوگیری می‌شود. همچنین قابلیت import داده نیز محدود شده و کاربر اجازه import کردن هر نوع داده‌ای را ندارد.

(FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4, FDP_ACC.1.1)

مثال‌ها:

1. مدیر میتواند برای تمامی کاربران، نقش جدید تنظیم کرده و یا آن‌ها را ویرایش کند. میتواند به کاربری نقش جدید اعمال کرده و یا نقش فعلی آن را حذف کند.(فرم مدیریت سطح دسترسی) .
2. سامانه هویت کاربر را پس از وارد کردن نام کاربری و رمز عبور شناسایی کرده و تمامی اطلاعت و فرم‌های مربوط به نقش کاربر که به آن‌ها دسترسی دارد را نمایش میدهد.
3. در صورت تغییر نقش کاربر، نشست فعال آن کاربر از بین رفته و به صفحه ورورد هدایت میشود.

4. سامانه صحت اطلاعات با اهمیت مانند فرم عملکرد کاربران را تشخیص میدهد و اگر اطلاعاتی توسط کاربری دستکاری شده باشد، آن رکورد به رنگ قرمز نمایش داده میشود.

- **شناسایی و احراز هویت**

سامانه کاربران را از طریق نام کاربری و رمز عبور ثبت شده شناسایی می‌کند. در صفحه ورود، کاربر می‌تواند با وارد کردن نام کاربری و رمز عبور به سامانه وارد شود. در صورت اشتباه وارد کردن رمز عبور، کپچا به کاربر نمایش داده می‌شود (برای جلوگیری از ورود ربات) و در صورت ورود مجدد رمز عبور اشتباه بیشتر از 5 بار، کاربر مربوطه توسط سامانه غیر فعال شده و برای فعال‌سازی نیاز به تایید مدیر می‌باشد. پس از ورود کاربر، سامانه کاربر را شناسایی کرده و اطلاعاتی را که با این کاربر تطابق دارد(دسترسی) ، نمایش می‌دهد. مدیر سامانه هنگام تعریف کاربر نمی‌تواند از رمز عبورهای ساده استفاده کند زیرا گذرواژه حتما باید شامل حروف کوچک، بزرگ، عدد و کاراکترهای خاص باشد.
همچنین در سامانه قابلیت فعالسازی احراز هویت چندگانه نیز وجود دارد. مدیر میتواند برای کاربر مورد نظر، این قابلیت را فعال نماید. با فعال شدن این قابلیت، کدی برای شماره همراه کاربر ارسال شده و با وارد کردن آن کد، در صورت صحیحی بودن، به سامانه وارد میشود.
(FIA_UID.1.1, FIA_UID.1.2, FIA_AFL.1.1, FIA_AFL.1.2, FIA_ATD.1.1, FIA_PMG_EXT.1.1,
(FIA_USB.1.1, FIA_USB.1.2 FIA_USB.1.3, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UAU.2.1

مثال‌ها:

1. کاربر قبل از ورود به سیستم اجازه‌ی کار با فرم‌ها و مشاهده اطلاعات را ندارد. برای ورود به سیستم باید از طریق نام کاربری و رمز عبور اقدام به احراز هویت کند.
2. در فرم تنظیمات صفحه ورود، مدیر میتواند تعداد دفعات وارد کردن رمز عبور اشتباه را مشخص کند. همچنین تعداد دفعات وارد کردن رمز اشتباه برای نمایش کپچا نیز قابل تنظیم است.
3. پس از شناسایی کاربر و احراز هویت موفق، سامانه اطلاعات و فرم‌هایی که کاربر جاری به آن‌ها دسترسی دارد را نمایش میدهد.
4. مدیر میتواند اطلاعات کامل کاربران و همچنین نقش‌های آنهارا مشاهده و مدیریت کند.
5. در فرم تنظیمات رمز عبور، مدیر میتواند پیچیدگی و طول رمز عبور را مشخص کند. حداقل طول مجاز 15 کاراکتر بوده و پیچیدگی رمز عبور میتواند شامل حروف کوچک، حروف بزرگ، اعداد و کاراکترهای

خاص(()*&^%$#@!) باشد. این پیچیدگی هنگام تغییر رمز عبور در فرم مدیریت کاربران اعمال میشود و اگر از پیچیدگی مناسب برخوردار نباشد، پیغام مناسبی نمایش داده میشود.

6. سامانه علاوه بر احراز هویت از طریق نام کاربری و رمز عبور، از ساز و کار ورود دو مرحله‌ای نیز پشتیبانی میکند. مدیر سیستم میتواند در قسمت مدیریت کاربران، به ازاء هر کاربر، ورود دو مرحله‌ای را فعال کند. هنگام ورود دو مرحله‌ای، کدی برای کاربر ارسال میشود و در صورت وارد کردن رمز درست، به سامانه وارد میشود.
7. مدیر میتواند در فرم مدیریت نشست‌های فعال، نشست فعال کاربران را تنظیم کند. میتواند حد آستانه برای نشست فعال به ازا هر کاربر مشخص کند. برای مثال کاربر user1 فقط میتواند 2 نشست فعال داشته باشد. همچنین مدیر میتواند تعداد کاربران مجاز برای ورود به سامانه را محدود کند.

- **مدیریت امنیت**

سامانه عملیات مدیریتی را فقط به مدیر ارشد یا کاربرانی که سطح دسترسی مدیر داشته باشند محدود کرده و کاربران عادی به واسطهای مدیرتی دسترسی ندارند. نقش‌های مختلفی می‌تواند در سیستم تعریف شود اما اکثرا نقش‌های **مدیر ارشد، مدیر سیستم، و کارشناس** به صورت پیشفرض تعریف می‌شود. در این قسمت مدیر می‌تواند کاربر جدید تعریف و یا کاربری را ویرایش و یا حذف نماید. همچنین به فرم مدیریت سطح دسترسی ، دسترسی دارد و می‌تواند سطح دسترسی کاربران را ویرایش کند. همچنین مدیر می‌تواند تعیین کند چه منویی به چه کاربری نمایش داده شود و یا این که چه کاربری اجازه حذف یا ویرایش چه اطلاعاتی را دارد.(FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_MTD.1.1(1), FMT_MTD.1.1(2), (FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2

مثال‌ها:

1. در قسمت امنیت، مدیر میتواند کاربران را مشاهده و یا ویرایش کند همچنین نقش‌های تنظیم شده برای هر کاربر قابل نمایش میباشد.
2. قسمت هایی که امنیت بالایی برخوردار هستند فقط توسط مدیر قابل مشاهده و ویرایش میباشد و هیچ کاربر با نقش دیگری قادر به مشاهده و ویرایش اینگونه اطلاعات نمیباشد. برای مثال فرم های مدیریت کاربران، مدیریت سطح دسترسی، عملکرد کاربران و ... فقط توسط کابر با نقش مدیر قابل دسترسی میباشد.
3. مدیر میتواند مشخص کند که چه منو/فرمی به چه کاربری نمایش داده شود. این کار باعث میشود که مدیر هر فرم را به ازا هر کاربر دسته بندی کرده و نمایش دهد.
4. در سامانه به صورت پیشفرض نقشی با نام کاربر میهمان وجود دارد که یک سری دسترسی های محدود و کمی دارد. این نقش زمانی به کابر اختصاص داده میشود که از طریق ورود شهروند به سامانه وارد شود.

5. ورود به صورت کاربر میهمان نیاز به وارد کردن رمز عبور و نام کاربری ندارد و سامانه آن کاربر را بر اساس نقش اعمال شده (کاربر میهمان) شناسایی میکند.
6. در این قسمت مدیر میتواند کاربران جدیدی در سیستم ثبت کرده و نقش‌هایی برای آن تنظیم کند.
7. در قسمت فرم تنظیمات IP ، مدیر میتواند محدوده مجاز برای IP را تنظیم کند و در صورت ورود با IP غیر مجاز، پیغام عدم دسترسی (403) نمایش داده میشود.

- **حفاظت از توابع امنیتی هدف ارزیابی**

در صورت رخداد شکست، سامانه تا حد امکان در وضعیت امنی قرار گرفته و به کاربر خطای معنا داری نمایش می‌دهد. برای مثال اگر ارتباط سامانه با پایگاه داده قطع شود، پیغام خطا "خطا در ارتباط با سرور" تولید شده و کاربر را مطّلع میکند (exception handling) . انتقال اطلاعات بین بخش‌های مختلف برنامه به صورت امن رد و بدل می‌شود و تا حد ممکن از شنود و ردیابی اطلاعات جلوگیری می‌شود. سامانه از طریق پروتکل‌های ارتباط امن مانند HTTPS و TLS نیز پشتیبانی کرده و در صورت فعال بودن این پروتکل‌ها، اختلال در کارکرد برنامه بوجود نمی‌آید.((FPT_FLS.1.1, FPT_ITT.1.1, FPT_TDC.1.1, FPT_TDC.1.2, FPT_STM.1.1

مثال‌ها:

1. در صورتی که خطای غیر قابل پیش بینی رخ دهد، سامانه پیغام مناسب به کابر نمایش میدهد. همچنین از نمایش کدها و یا نام توابع امنیتی در پیغام خطا جلوگیری میشود.
2. هنگام ارتباط با دیتابیس و یا ارتباط با پنل SMS ، این ارتباط به صورت امن برقرار میشود و اطلاعات مورد نیاز به صورت رمز شده رد و بدل میشود. این مورد باعث بالا بردن امنیت داده‌های انتقالی میشود.

- **تخصیص منابع**

در صورت بروز خطا یا شکست نرم افزاری، سامانه پیغام‌های معنادار و قابل درکی تولید می‌کند که کاربر متوجه خطا شود. شکست‌ها به دسته‌های مختلفی تقسیم می‌شود که عبارتند از:

شکست عملیاتی نرم افزار هنگام ثبت یک درخواست در سامانه (crud): نمایش پیغام معنا دار

عدم اتصال به پایگاه داده: نمایش پیغام به کاربر(سامانه از حالت standby خارج شده و قادر به پردازش درخواست کاربران نمی‌باشد).(FRU_FLT.1.1)

در صورت بروز خطا یا شکست نرم افزاری، سامانه از اطلاعات حفاظت کرده و مانع از بین رفتن اطلاعات میشود. همچنین خللی در هنگام کار با سیستم بوجود نمی‌آید و فقط پیغام خطا به کاربر نمایش داده میشود.

برای مثال اگر ارتباط با دیتابیس قطع شـود، خطایی با عنوان خطا در ارتباط با سـرور نمایش داده میشـود و یا اگر عبارات غیر مجاز در کادر متنی وارد شود، سیستم آن را شناسایی کرده و پیغام "استفاده از کاراکتر غیرمجاز" نمایش داده میشود.

- **دسترسی به هدف ارزیابی**

سامانه به صورت پیشفرض، محدودیتی برای تعداد نشست توسط کاربر یکسان اعمال نمی‌کند و کاربر می‌تواند از طریق چند سیستم(نشست) وارد سامانه شود. اما قابلیتی وجود دارد که با فعالسازی آن، کاربر تنها از طریق یک سیستم(نشست) می‌تواند به سیستم وارد شود. اگر کاربر در سیستم وارد شده باشد و بخواهد از طریق نشست دیگر، مجددا وارد سیستم شود، در صفحه ورود پیغامی با عنوان "کاربری با این اطلاعات در سیستم لاگین شده است" نمایش داده می‌شود و از ورود مجدد جلوگیری می‌کند.
سامانه برای هر نشست محدودیت زمانی در نظر می‌گیرد و به صورت خودکار پس از بیست دقیقه، نشست جاری را از بین برده و به صفحه ورود هدایت می‌شود. همچنین خود کاربر نیز پس از ورود می‌تواند با استفاده از گزینه خروج(sign out) به نشست جاری پایان دهد. همچنین پس از ورود موفق کاربر به سیستم، کاربر میتواند 3 نشست موفق آخر و 1 نشست ناموفق آخر را مشاهده کند. همچنین تعداد کل نشست ناموفق نیز قابل مشاهده میباشد.
(FTA_TAH.1.1, FTA_TAH.1.2, FTA_TAH.1.3, FTA_TSE.1.1, FTA_MCS.1.1, FTA_MCS.1.2, FTA_SSL.3.1, FTA_SSL.4.1)

مثال‌ها:

1. در قسمت پیشینه احراز هویت، کابر میتواند تعداد نشست‌های فعال/غیر فعال را مشاهده کند. همچنین اطلاعاتی مانند IP، تاریخ و زمان قابل مشاهده میباشد.
2. در قسمت مدیریت نشست فعال ، مدیر میتواند محدودیت‌هایی را برای تعداد نشست فعال برای هر کاربر و تعداد کاربران مجاز برای ورود به سامانه را تنظیم کند. برای مثال، اگر محدودیت نشست فعال برای هر کاربر برابر با 1 باشد، کاربری با نام کاربری test فقط میتواند 1 نشست فعال داشته باشد.
3. نشست جاری در صورت عدم فعالیت پس از 20 دقیقه به صورت خودکار از بین میرود که این زمان را میتوان در قسمت تنظیمات سامانه تغییر داد.
4. کاربر وارد شده به سیستم از طریق منو خروج میتواند به نشست جاری خود خاتمه دهد.
5. در فرم تنظیمات IP مدیر میتواند برای IP محدوده مجاز تعیین کند و از دسترسی به IP های غیر مجاز به سامانه جلوگیری کند.

- **کانال‌ها و مسیرهای مورد اعتماد**

سامانه در صورت فراهم بودن زیر ساخت لازم با استفاده از پروتکل امن (TLS,HTTPS) بدون هیچ مشکل و محدودیتی به کار خود ادامه می‌دهد و موجب بروز اختلال در سیستم نشده و باعث افزایش امنیت داده‌های انتقالی بین اجزاء برنامه می‌شود. این امر باعث جلوگیری از فیشینگ اطلاعات میشود(FTP_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3)

در صورت برقراری ارتباط خارجی (پیام کوتاه)، سامانه از کانال‌های امن TLS و SSL استفاده میکند تا اطلاعات ارسال شده قابل فیشینگ نباشند. همچنین ارتباط TLS قدیمی با سیستم امکانپذیر نیست و سامانه از برقراری ارتباط جلوگیری میکند.

برای مثال، هنگام ارسال رمز عبور در ثبت نام یا ورود دو مرحله‌ای، اطلاعات ارسال شده از طریق کانال امن صورت میگیرد.

- **صحت داده کاربری**

در صورتی که اطلاعات مهم و حساس از طریق دیتابیس توسط یک کاربر تغییر کند، سامانه صحت اطلاعات را تشخیص داده و برای مدیر یک sms ارسال میکند که دستکاری غیر مجاز رخ داده است. همچنین لاگ مربوط به دستکاری غیر مجاز در فرم عملکرد کاربران با رنگ قرمز نمایش داده میشود. اگر اطلاعات تغییر کرده باشد، مقدار قبلی و مقدار جدید لاگ میشود. همچنین IP سرور دیتابیس و ساعت آن نیز ذخیره میشود. اگر اطلاعات حذف یا اضافه شده باشد، شناسه آن رکورد ذخیره میشود، برای مثال : رکورد با id = 5 اضافه شد. صحت اطلاعات هر رکورد از طریق فیلد hash در همان جدول شناسایی میشود. ابتدا رکورد به json تبدیل شده و سپس هش میشود.
(FDP_SDL2.1 , FDP_SDL2.2)

- **مسیر امن**

سامانه به دلیل استفاده از SSL ، ارتباط امنی را با کابران ایجاد میکند که حملات فیشینگ را تا حد زیادی کاهش میدهد. برای مثال اطلاعات حساس مانند رمز عبور و ... چون از کانال امن رد و بدل میشوند، ایمن هستند. همچنین برای ارتباط با سرور خارجی که در سامانه فقط سرور sms میباشد، از TLS1.1 و TLS1.2 استفاده میکند که باعث میشود اطلاعات ارسالی رمزنگاری شده و قابل واکشی توسط هکر نباشد. همچنین certificate مربوط به سرورsms نیز بررسی میشود که اگر مشکلی در certificate وجود داشت، ارتباط برقرار نمیشود.
(FTP_TRP.1.1 , FTP_TRP.1.2 , FTP_TRP.1.3)

- **الزامات پروتکل X509**

سامانه تنها برای ارسال SMS با سرور خارجی در ارتباط است. در این حالت سرور ما نقش یک کلاینت را بازی میکند. در سامانه از CRL استفاده شده است. هنگام ارسال SMS از کانال امن TLS 1.1 و 1.2 استفاده میکند. همچنین اطلاعات certificate سرور خارجی برای امنیت بیشتر بررسی میشود. اگر گواهینامه منقضی شده باشد یا اطلاعات آن با اطلاعات سرور یکسان نباشد و یا به هر دلیلی مشکلی در آن وجود داشته باشد، تایید نشده و ارتباط با سرور خارجی برقرار نمیشود. همچنین اگر به هر دلیلی ، گواهینامه revoke شده بود، ارتباط برقرار نخواهد شد.
(FIA_X509_EXT.1.1, FIA_X509_EXT.1.2, FIA_X509_EXT.2.1, FIA_X509_EXT.2.2)

- **حفاظت از اطلاعات باقیمانده در منابع**

در سامانه هنگام حذف کردن یک سری از اطلاعات ، سایر داده های مربوط به آن نیز حذف خواهد شد تا از پر شدن حافظه جلوگیری شود. برای مثال اگر کاربر سامانه یک درخواستی را به همراه یک تصویر و یا یک فایل صوتی ثبت نماید، اگر مدیر تصمیم بگیرد که این درخواست را حذف نماید، علاوه بر حذف شدن درخواست، فایل های ضمیمه شده به آن درخواست نیز از سامانه به صورت کامل حذف خواهد شد.

(FDP_RIP.2.1)