به نام خدا

سند هدف امنیتی

سرویا / وندیا – نسخه ۱/۱۰

گروه فناوری پرند

آبان ۱۴۰۲

۱/۰

فهرست

۱ معرفی

۱/۱ مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی سرویا / وندیا – نسخه ۱/۱۰
نسخه	۱/۰
تاریخ	۱۴۰۲-۰۸
نویسندگان	واحد راهکار و محصول و واحد فنی گروه فناوری پرند

نام شرکت	گروه فناوری پرند
نام محصول	سرویا - وندیا
نوع محصول	برنامه های کاربردی تحت شبکه
نسخه‌ی محصول	۱/۱۰

حداقل نیازمندی نرم افزاری/سخت‌افزاری/میان‌افزاری محصول

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

سخت‌افزار/نرم افزار/میان‌افزار	حداقل الزامات
مدل و نسخه سیستم عامل	Microsoft Windows Server 2019
مدل و نسخه وب سرویس	Microsoft IIS 10.0
مدل و نسخه پایگاه داده	Microsoft SQL Server 2019
مدل و نسخه نرم افزار پایه	Microsoft .NET Framework 4.7.x
مرورگر کلاینت	Firefox / Google Chrome Latest Update
پردازنده هر سرور	High End Xeon (Gold / Platinum)
حافظه اصلی هر سرور	32GB – 64GB
فضای دیسک هر سرور	100GB – 200GB

۲ ادعای انطباق

در این قسمت باید انطباق سند هدف ارزیابی با موارد مطرح شده در جداول زیر مشخص شود، برای اطلاعات بیشتر جهت تکمیل این قسمت به بخش ۱/۲ از سند «راهنمای نوشتن سند هدف امنیتی» مراجعه شود.

۱/۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
نام پروفایل حفاظتی	Network Based Applications v1.1
سطح تضمین امنیتی	EAL1

۲/۲ شرح محصول

نرم افزار سرویا / وندیا یک راهکار مدیریت خدمات فناوری اطلاعات، مدیریت امنیت اطلاعات و حاکمیت اطلاعات و فناوری اطلاعات است که مبتنی بر بهین روش های ITIL، ISMS و COBIT می باشد. این نرم افزار پوشش دهنده کلیه فرآیندهای بهین روش های مذکور بوده و دارای اجزاء و ماژول های اصلی ذیل می باشد:

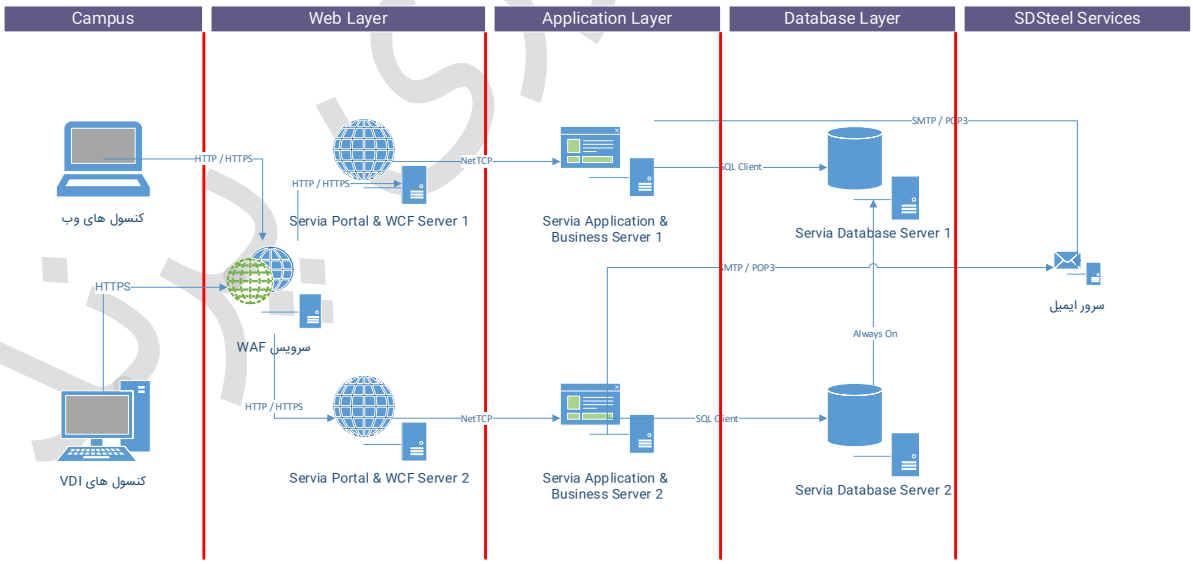
- مدیریت پیشخوان خدمت
- مدیریت دارایی و پیکربندی
- مدیریت پروژه و تغییر
- مدیریت سطح خدمت
- مدیریت منابع و زمان
- مدیریت خرید و انبار
- مدیریت مالی و صورتحساب

۱/۲/۲ حوزه فیزیکی

عناصر سخت‌افزاری و نرم افزاری مورد استفاده در جدول زیر مشخص گردیده است:

عناصر محصول	شماره مدل یا نسخه
پایگاه داده	Microsoft SQL Server 2019
چارچوب .NET	Microsoft .NET Framework 4.7.x

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



شکل ۱: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

۲/۲/۲ حوزه منطقی

کارکردها	توصیف
نقش های کارکردی	این نقش ها برای تبیین دسترسی کاربران به اشیاء موجود در سیستم از قبیل پنجره ها، کنترل ها، فیلدها، داشبوردها، منوها، تب ها و ... مورد استفاده قرار می گیرد.
نقش های محرمانگی	این نقش ها برای تبیین دسترسی کاربران به هر یک از رکوردهای اطلاعاتی مندرج در سیستم مورد استفاده قرار می گیرد.
گروه های کاربری و کاربران	کاربران برای ورود به سامانه با عضویت در گروه های کاربری و تخصیص نقش به گروه / کاربر دسترسی های لازم را خواهند داشت.
لاگ ممیزی امنیتی	این لاگ، برای کنترل دسترسی به اجزاء مختلف سیستم، ورود و خروج، دریافت فایل ها و خروجی ها و ... مورد استفاده قرار می گیرد.
پیکربندی امنیتی	این بخش با توجه به حداقل الزامات مورد انتظار، امکان افزودن پیچیدگی های امنیتی به سامانه، از جمله روز عبور را برای راهبر فراهم می سازد.
ساز و کار احراز هویت	این نرم افزار از طریق روش های متفاوت Local Authentication، Windows Authentication و LDAP Authentication احراز هویت را انجام می دهد.

۳ مسائل امنیتی

۱/۳ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیداکند. این دسترسی می تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم می تواند با سود بردن از نقضهای امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری آزمون بر روی سیستم واقعی به محصول دسترسی پیدا کند. همچنین مهاجم می تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده ها می توانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می تواند با دسترسی به داده ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردها، مستندات و داده های حفاظت شده توسط محصول می تواند بدون مجوز تغییر یابند. مهاجم می تواند با گمراه نمودن مدیر سیستم، واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می تواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می دهد که صحت رکوردها و مستندات تضمین شده نیست. مهاجم ممکن است درصدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیداکند.

تهدیدات	توضیحات
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول است تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می تواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می تواند با اضافه کردن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه کند.
افشای اطلاعات	داده های محرمانه که توسط محصول محافظت می شوند می تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می تواند سبب گردد محصول در یک بازه زمانی غیرقابل دسترسی یا بلا استفاده گردد. این امر معمولا با ارسال درخواست های بسیار در یک بازه زمانی کوتاه صورت میگیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده ای از حمله شامل ارسال درخواست های بسیار از یک رنج IP مشخص است که به نام جمله DoS شناخته می شود. نوع دیگر پیشرفته تر حملهDDoS است که از BOTNET استفاده می کند و محدودیتی بر روی آدرس IP ورودی ندارد.
داده های ورودی مخرب	مهاجم می تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد کند. با استفاده از این تهدید، مهاجم می تواند به داده کاربر خاص دسترسی پیدا کند، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم می تواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاترکند.
شنود شبکه	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می شود تا انتقال داده های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده های رد وبدل شده بین محصول و یک یا چندکاربر از راه دور و یا محلی است. به عنوان مثال می توان به موردی اشاره کرد که در آن یک کاربر تلاش می کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می کند.

۲/۳ خط مشی امنیتی

خط مشی ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردهامحافظت شده هستند و معمولا به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می گیرند.
پیکربندی مناسب	پیکربندی پیش فرض محصول و مؤلفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوری که مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری Root پیش فرض، خطاهای پیش فرض و صفحات۴۰۴، مقادیر احراز هویت پیش فرض، نام کاربری پیش فرض، پورت های پیش فرض، صفحات پیش فرض که اطلاعات داخلی همچون شماره نسخه را آشکارمی نمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانی که محصول یا هرمؤلفه تعاملی

خط مشی ها	توضیحات
	به طور گسترده مورد استفاده قرار میگیرد؛ بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی میتوان از حمله ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳/۳ فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال می نمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می نمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ می نمایند.
محیط امن	فرض شده است که تمام پیشبینی های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدام مناسبی صورت میگیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگرمؤلفه های سخت افزاری دارای پشتیبان مناسبی هستند و بنا بر وجود نسخه پشتیبان هیچ داده ای از دست نمی رود. همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی دهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانالهای ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می شوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می شود.

۴ اهداف امنیتی

۱/۴ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکوردکند. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت کند. محصول باید به کاربران

هدف امنیتی	توضیحات
	مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه کند.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت کند و مطابق با نقش و مجوزهایشان مجاز کند. محصول باید برای احراز هویت کاربر، قوانینی تعریف کند طوری که کاربران را ملزم به استفاده از کلمه های عبور قدرتمند کند. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف کند. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می کند. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم کند. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احراز هویت کند. از جمله ساز و کارها می توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت بر اساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده های غیرمجاز را کنترل و مدیریت کند. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنجIP تعریف شده می تواند بیانگر حملهDoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم کندکه به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد. همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده کند.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل کند و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن وکارآمدسیستم فراهم کند. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش ها و مجوزهایی تنظیم کند.
مدیریت خطا	محصول باید صورت امن وکارآمد سازوکار مدیریت خطا فراهم کند. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ کند.
مدیریت داده های باقی مانده	محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می گردد.
ارتباط امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۲/۴ اهداف امنیتی برای محیط عملیاتی

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

۵ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید داده ممیزی ۱	FAU_GEN.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	مرتبط نمودن هویت کاربر به رویداد ۱	FAU_GEN.2.1
۴	بازبینی داده ممیزی ۱	FAU_SAR.1.1
۵	بازبینی داده ممیزی ۲	FAU_SAR.1.2
۶	بازبینی داده ممیزی محدود ۱	FAU_SAR.2.1
۷	بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.3.1
۸	انتخاب داده ممیزی ۱	FAU_SEL.1.1
۹	ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۱۰	ذخیره سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۱۱	اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1
۱۲	پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱	FAU_STG.4.1
۱۳	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۴	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۵	خط مشی کنترل دسترسی ۱	FDP_ACC.1.1
۱۶	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۱۷	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۱۸	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۱۹	عملیات کنترل دسترسی ۴	FDP_ACF.1.4
۲۰	حفاظت کامل از اطلاعات باقیمانده در منابع ۱	FDP_RIP.2.1
۲۱	ورود داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.2.1
۲۲	ورود داده کاربری به محصول با مشخصه امنیتی ۲	FDP_ITC.2.2
۲۳	ورود داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.2.3
۲۴	خروج داده کاربری از محصول با مشخصه امنیتی ۱	FDP_ETC.2.1
۲۵	خروج داده کاربری از محصول با مشخصه امنیتی ۲	FDP_ETC.2.2
۲۶	خروج داده کاربری از محصول با مشخصه امنیتی ۴	FDP_ETC.2.4
۲۷	صحت داده کاربری ذخیره شده ۲	FDP_SDI.2.1
۲۸	صحت داده کاربری ذخیره شده ۳	FDP_SDI.2.2
۲۹	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۳۰	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۱	تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۳۲	مدیریت کلمه عبور	FIA_PMG_EXT.1.1
۳۳	احراز هویت کاربر ۱	FIA_UAU.1.1
۳۴	احراز هویت کاربر ۲	FIA_UAU.1.2
۳۵	سازوکار احراز هویت چندگانه ۱	FIA_UAU.5.1
۳۶	سازوکار احراز هویت چندگانه ۲	FIA_UAU.5.2
۳۷	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۳۸	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۳۹	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۴۰	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۴۱	مدیریت مشخصه های امنیتی ۱	FMT_MSA.1.1
۴۲	مدیریت داده محصول ۱	FMT_MTD.1.1
۴۳	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۴۴	نقش های امنیتی ۱	FMT_SMR.1.1
۴۵	نقش های امنیتی ۲	FMT_SMR.1.2
۴۶	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۴۷	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۴۸	سازگاری داده امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۴۹	مهرهای زمانی ۱	FPT_STM.1.1
۵۰	به روزرسانی امن ۲	FPT_TUD_EXT.1.2
۵۱	به روزرسانی امن ۳	FPT_TUD_EXT.1.3
۵۲	تحمل خطا ۱	FRU_FLT.1.1
۵۳	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۴	خاتمه دادن به نشست ها توسط محصول ۱	FTA_SSL.3.1
۵۵	خاتمه دادن به نشست ها توسط کاربر ۱	FTA_SSL.4.1
۵۶	سوابق دسترسی به محصول ۱	FTA_TAH.1.1
۵۷	سوابق دسترسی به محصول ۲	FTA_TAH.1.2
۵۸	سوابق دسترسی به محصول ۳	FTA_TAH.1.3
۵۹	برقراری نشست ۱	FTA_TSE.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۰	مسیر امن ۱	FTP_TRP.1.1
۶۱	مسیر امن ۲	FTP_TRP.1.2
۶۲	مسیر امن ۳	FTP_TRP.1.3
الزامات مربوط به پیوست اول		
۶۳	تولید کلید رمزنگاری ۱	FCS_CKM.1.1
۶۴	تخریب کلید رمزنگاری ۱	FCS_CKM.4.1
۶۵	عملیات رمزنگاری ۱ -رمزنگاری و رمزگشایی ۱ (۳)	FCS_COP.1.1(3)
۶۶	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
الزامات مربوط به پیوست دوم		
۶۷	الزامات پروتکل HTTPS (۱)	FCS_HTTPS_EXT.1.1
۶۸	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۶۹	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۷۰	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۷۱	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۷۲	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۷۳	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۷۴	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۷۵	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۷۶	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۷۷	الزامات پروتکل TLS Server / احراز هویت (۴)	FCS_TLSS_EXT.2.4
۷۸	الزامات پروتکل TLS Server / احراز هویت (۵)	FCS_TLSS_EXT.2.5
۷۹	الزامات پروتکل TLS Server / احراز هویت (۶)	FCS_TLSS_EXT.2.6
۸۰	الزامات پروتکل X509 (۱) / ابطال	FIA_X509_EXT.1.1/Rev
۸۱	الزامات پروتکل X509 (۱) / ابطال	FIA_X509_EXT.1.2/Rev
۸۲	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1

۱/۵ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**

محصول باید بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید کند:

- آغاز و اتمام توابع ممیزی؛
- تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول ۱ آمده است.

جدول۱- لیست رویدادهای قابل ممیزی

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

شماره الزام	نام الزام		
		ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)	
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر		ثبت شکست انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
مدیریت مشخصه های امنیتی		تمامی تغییرات بر روی مقادیر مشخصه های امنیتی (پایه)	
مدیریت داده های محصول ۱ - مدیر سیستم		تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه)	
مدیریت داده های محصول ۱ - کاربر عادی، واردکننده داده		تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه)	
عملیات رمزنگاری ۱ (۱)		شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه های موجودیت های فعال و غیرفعال (پایه)	
عملیات رمزنگاری ۱ (۲)		شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه های موجودیت های فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی ۱		درخواستهای موفقیتآمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	
ورود داده های کاربری به محصول با مشخصه امنیتی		ورود داده کاربری موفقیت آمیز، شامل هرگونه مشخصه های امنیتی (حداقل) تمامی تلاشها برای وارد کردن داده های کاربری، شامل هرگونه مشخصه های امنیتی (پایه)	
خروج داده های کاربری از محصول با مشخصه امنیتی		خروج اطلاعات به طور 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)	
نقش های امنیتی		ثبت تغییرات در گروههای کاربری که بخشی از یک نقش است (حداقل)	
سازگاری داده های امنیتی بین محصول و موجودیت امن		ثبت استفاده موفق از سازوکار سازگاری داده های محصول (حداقل)	

شماره الزام	نام الزام
	ثبت استفاده از سازوکار سازگاری داده های محصول (پایه)
حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)
تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت های در حال قطع شدن محصول که به دلیل شکست است (پایه)
برقراری نشست ۱	ثبت منع آغاز نشست به دلیل سازوکار آغاز نشست (حداقل) ثبت تمامی تلاشها در آغاز نشست کاربر (پایه)
محدودیت بر روی چندین نشست همزمان	ثبت رد یک نشست مبتنی بر محدودیت نشست های همزمان (حداقل)
خاتمه دادن به نشست ها	ثبت خاتمه دادن به یک نشست بیکار توسط سازوکار قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)

۲	**تولید داده ممیزی ۲**

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 کاربر، کلاینت مورد استفاده، شناسه کاربری، زمان و تاریخ انجام فعالیت، محتوای داده ممیزی]

۳	**مرتبط نمودن هویت کاربر به رویداد ۱**

برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است را شناسایی و ثبت کند.

۴	**بازبینی داده ممیزی ۱**

محصول باید امکان خواندن [فهرستی از اطلاعات ممیزی] از کل رکوردهای ممیزی را برای [کاربران با نقش مجاز] فراهم نماید.

۵	**بازبینی داده ممیزی ۲**

محصول باید رکوردهای ممیزی را طوری فراهم کند که کاربر بتواند آنها را درک و اطلاعات این رکوردها را تفسیر کند.

۶	**بازبینی داده ممیزی محدود ۱**
محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.	
۷	**بازبینی داده ممیزی قابل انتخاب ۱**
محصول باید امکان انجام [جستجو و مرتب سازی] رکوردهای ممیزی را به نحوی فراهم کند که کاربر مجاز بتواند آن رکوردها را بر اساس [نوع رویداد، آدرس IP کاربر، حساب کاربری، تاریخ و زمان انجام فعالیت، کلاینت مورد استفاده، محتوای داده ممیزی] مرتب کند.	
۸	**انتخاب داده ممیزی ۱**
محصول باید قادر باشد بر اساس مشخصه های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه ای از رخدادها را جهت ممیزی شدن، انتخاب کند: • [نوع رخداد] • [آدرس IP کاربر، کلاینت مورد استفاده]	
۹	**ذخیره سازی رویدادهای ممیزی ۱**
محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را، از حذف غیرمجاز حفاظت کند.	
۱۰	**ذخیره سازی رویدادهای ممیزی ۲**
محصول باید قادر به [جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره سازی آنها باشد.	
۱۱	**اقدامات لازم در زمان از دست رفتن داده ممیزی ۱**
محصول در صورت تجاوز دنباله ممیزی از [تعداد رکوردهای ثبت شده] باید با استفاده از [پیام داخل سیستم به مدیر سامانه] مطلع کند.	
۱۲	**پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱**
محصول در صورت پر شدن دنباله ممیزی، باید [رویدادهای ممیزی را نادیده بگیرد] و [یا پیام داخل سیستم به مدیر سامانه را ارسال نماید]	

۲/۵ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۳	**عملیات رمزنگاری ۱ (۱)**
محصول باید [برای وارسی صحت داده های ممیزی و داده های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [GCM] و اندازه کلید رمزنگاری [۱۲۸ و ۲۵۶ بیت] اجرا شود که مطابق با [NIST SP 800-38D] باشد.	
۱۴	**عملیات رمزنگاری ۱ (۲)**
محصول باید [برای تولید داده درهم سازی] بر اساس مجموعه الگوریتم های رمزنگاری مشخص [SHA-256 و SHA-384] و اندازه کلید رمزنگاری [۲۵۶ و ۳۸۴ بیت] اجرا شود که مطابق با [ISO/IEC 10118-3:2004] باشد.	

۳/۵ کلاس حفاظت از داده کاربری

شماره الزام	نام الزام
۱۵	**خط مشی کنترل دسترسی ۱**
محصول باید [خط مشی های کنترل دسترسی] را بر روی موارد زیر اعمال کند:] • موجودیت فعال: [مدیر سیستم، کاربر عادی] • موجودیت غیرفعال: ○ رکوردها، مستندات و فرا-داده[1] ○ داده متعلق به کاربران ○ داده احراز هویت • عملیات: ○ ایجاد موجودیت غیرفعال جدید ○ حذف موجودیت غیرفعال ○ تغییر دسترسی ها به موجودیت غیرفعال ○ عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال [	
۱۶	**عملیات کنترل دسترسی ۱**
محصول باید [خط مشی های کنترل دسترسی] را با توجه به موارد زیر بر روی موجودیت های غیرفعال اعمال کند:]	

[1] Metadata

شماره الزام	نام الزام
• هویت کاربر • نقش ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند]	
۱۷	**عملیات کنترل دسترسی ۲**
محصول باید قوانین زیر را اجرا کند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز کند: [عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به موجودیت غیرفعال را با نقش موجودیت فعال از طریق نقش های محرمانه مرتبط نماید.]	
۱۸	**عملیات کنترل دسترسی ۳**
محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: [• کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند. • کاربران با مجوز عادی به رکوردهای لازمه بر اساس نقش محرمانگی اعطاء شده، دسترسی دارند.]	
۱۹	**عملیات کنترل دسترسی ۴**
محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری کند: [• تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[۲] از پیش تعریف شده،]	
۲۰	**حفاظت کامل از اطلاعات باقیمانده در منابع ۱**
محصول باید تضمین کند در هنگام [آزادسازی منابع از] تمام موجودیت های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.	
۲۱	**ورود داده کاربری به محصول با مشخصه امنیتی ۱**
محصول باید هنگام دریافت داده کاربری، [خط مشی کنترل دسترسی] را اعمال کند.	

[۲] Threshold

۲۲	**ورود داده کاربری به محصول با مشخصه امنیتی ۲**
محصول باید از مشخصه های امنیتی مرتبط با داده کاربری هنگام وارد کردن داده استفاده کند. مشخصات امنیتی شامل مواردی از این قبیل است: نوع داده، حجم و اندازه فایل، فرمت فایل، تعداد دفعات Import و از این قبیل موارد.	
۲۳	**ورود داده کاربری به محصول با مشخصه امنیتی ۳**
محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه های امنیتی و داده کاربری دریافت شده، فراهم می کند.	
۲۴	**خروج داده کاربری از محصول با مشخصه امنیتی ۱**
محصول باید هنگام خروج داده کاربری به بیرون[۳] [خط مشی کنترل دسترسی] را اعمال کند.	
۲۵	**خروج داده کاربری از محصول با مشخصه امنیتی ۲**
محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون از محصول)، مشخصه های امنیتی مرتبط با داده کاربری را نیز انتقال دهد.	
۲۶	**خروج داده کاربری از محصول با مشخصه امنیتی ۴**
محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال کند: [مدیر سیستم باید خروج رکوردها را محدود کند، به طوری که کاربران محصول، قادر به خروج بدون هدف داده به بیرون از آن (خارج از محصول) نباشند.]	
۲۷	**صحت داده کاربری ذخیره شده ۲**
محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص [خطاهای صحت داده] داده های رکورد و داده های ممیزی را بر اساس مشخصه های [درهم شده[۴] داده های کاربری ذخیره شده] پایش کند.	
۲۸	**صحت داده کاربری ذخیره شده ۳**
هنگام تشخیص خطای صحت داده، محصول باید [پیشگیری از دسترسی غیر مجاز با کنترل دسترسی ها و پیکربندی امن] را صورت دهد.	

[۳] Export user data
[۴] Hash

۴/۵ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۲۹	**مدیریت احراز هویت ناموفق**
محصول باید بتواند با استفاده از [یک عدد مثبت قابل تنظیم توسط مدیر] ، تلاشهای ناموفق احراز هویت مرتبط با [ورود ناموفق به پورتال کاربران، پورتال کارشناسان و سامانه مدیریتی] را تشخیص دهد.	
۳۰	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاشهای ناموفق صورت گرفته برای احراز هویت [بیشتر از حد تعیین شده رسید]، محصول باید[غیر فعال کردن حساب کاربری که فعال شدن آن توسط مدیر سیستم انجام می شود] را اجرا کند که باعث پیچیده تر کردن عمل احراز هویت مجدد کاربر شود.	
۳۱	**تعریف مشخصات کاربر ۱**
محصول باید مشخصه های امنیتی زیر را برای هر کاربر نگهداری نماید: [• شناسه کاربر • داده احراز هویت • نقش کاربر • وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)]	
۳۲	**مدیریت کلمه عبور**
محصول باید قابلیت های مدیریت کلمه عبور را که در زیر ذکر شده اند برای کلمه های عبور مدیریتی فراهم کند: ۱) کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: ["@"، "#"، "$"، "٪"، "^"، "!" "&"،"("، "*" , ")"] باشد. ۲) حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.	
۳۳	**احراز هویت کاربر ۱**
محصول باید پیش از احراز هویت کاربر، اجازه اقدامات میانی زیر را به کاربر دهد: [• هیچ اقدامی]	

۳۴	احراز هویت کاربر ۲

محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احراز هویت نماید.

۳۵	سازوکار احراز هویت چندگانه ۱

محصول باید به منظور احراز هویت کاربر سازوکارهای زیر را فراهم آورد:

]

- نام کاربری و کلمه عبور
- [Active Directory]

[

۳۶	سازوکار احراز هویت چندگانه ۲

محصول باید هر کاربر متقاضی احراز هویت را مطابق [کاربران از راه دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه (مانند Dual factor authentication) استفاده کند، [OTP یا توکن]] احراز هویت کند.

۳۷	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱

محصول باید مشخصه های امنیتی زیر را برای کاربر فعال نگهداری کند:

]

- شناسه کاربر
- نقش ها و یا مجموعه دسترسی های کاربر به قسمت های مختلف برنامه
- پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)

[

۳۸	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲

محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می کند، اعمال کند:

]

- زمانی که یک نشست جدید برقرار میشود، اعتبار نشست های 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.)
- اطلاعات پیشینه احراز هویت باید به روزرسانی گردد

[

۳۹	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳

محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه های امنیتی کاربر فعال اعمال کند:

[هیچ تغییری در طول نشست فعال مجاز نیست]

۵/۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۰	**مدیریت کارکرد در محصول ۱**
محصول باید امکان [تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] توابع [تمام کارکردهای مربوط به مدیریت محصول] را به [مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود کند.	
۴۱	**مدیریت مشخصه های امنیتی ۱**
محصول باید با اعمال [خط مشی کنترل دسترسی]، امکان تغییر پیش فرض، [پرس وجو، تغییر، حذف، [تغییر پیش فرض]] مشخصه های امنیتی [شناسه کاربر، نقش ها و یا مجموعه دسترسی های کاربر به قسمت های مختلف برنامه، پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)] را به [مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود کند.	
۴۲	**مدیریت داده محصول ۱**
محصول باید امکان [تغییر پیش فرض، پرس وجو، تغییر، حذف، پاک نمودن، [مقداردهی، مشاهده]] [داده های ممیزی و داده های احراز هویت و کلیدها] را به [مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود کند.	
۴۳	**کارکردهای مدیریتی محصول ۱**

محصول باید قادر به انجام [کارکردهای مدیریتی که در جدول زیر آمده است] باشد:

بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دست رفتن داده ممیزی	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده های ممیزی	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه های مورد استفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده درمنابع	انتخاب هنگام اجرای حفاظت از اطلاعات باقیمانده (برای مثال، تخصیص و یا آزادسازی) که می تواند 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

شماره الزام	نام الزام	
	صحت داده های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می تواند قابل پیکربندی باشد.
	مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاشهای ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.
	تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد.
	مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت ها برای تنظیم کلمه عبورها
	احراز هویت کاربر	مدیریت داده های احراز هویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احراز هویت کاربر انجام می شوند.
	سازوکار احراز هویت چندگانه	مدیریت سازوکارهای احراز هویت مدیریت قوانین مرتبط با احراز هویت
	شناسایی کاربر	مدیریت شناسایی کاربران مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می تواند قبل از شناسایی کاربر انجام دهد.
	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز می تواند مشخصه های امنیتی موجودیت های فعال پیش فرض را تعریف و تغییر دهد.
	مدیریت مشخصه های امنیتی	مدیریت گروهی از نقش هایی که با مشخصه های امنیتی در تعامل هستند.
	مقداردهی اولیه مشخصه ها	مدیریت گروهی از نقش هایی که مقادیر اولیه را مشخص میکنند. مدیریت مقادیر پیش فرض برای کنترل دسترسی محصول
	مدیریت داده های محصول ۱ -مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده های محصول
	مدیریت داده های محصول ۱ -کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده های محصول
	نقش های امنیتی	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
	محدودیت بر روی چندین نشست همزمان	مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر
	برقراری نشست	مدیریت شرایط آغاز نشست توسط مدیر مجاز
	خاتمه دادن به نشست ها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش فرض غیرفعال بودن کاربر که نشست خاتمه یابد.
۴۴	**نقش های امنیتی ۱**	
نقش های زیر در محصول باید تعریف شده باشد: [مدیر سیستم، کاربر عادی، [کاربر پیشرفته، درخواست کننده، کارشناس، مدیر، مالک]]		

۴۵	**نقش های امنیتی ۲**
محصول، باید قادر به مرتبط نمودن کاربران با نقش ها و دسترسی های مجاز تعریف شده باشند.	

۶/۵ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	نام الزام
۴۶	**حفظ وضعیت امن در زمان شکست ۱**
محصول باید در زمان رخداد انواع شکست های زیر، وضعیت امن را حفظ نمایند: [شکست های نرم افزاری، شکست های سخت افزاری]	
۴۷	**انتقال داده امنیتی در داخل محصول ۱**
محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخش های مجزای خود که باهم ارتباط دارند، محافظت کند.	
۴۸	**سازگاری داده امنیتی بین محصول و موجودیت امن ۱**
محصول در صورت استفاده از محصولات امن IT ، باید تفسیر سازگار [داده های احراز هویت، و بدون ذخیره سازی رمز عبور برای مثال از طریق Kerberos در ارتباط با Active Directory] را در زمان اشتراک گذاری داده امنیتی بین خود و دیگر محصولات امن IT ، فراهم آورد.	
۴۹	**مهرهای زمانی ۱**
محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و سازوکار کارکردی صحیح برطرف کند.	
۵۰	**به روزرسانی امن ۲**
محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولیدکننده محصول فراهم کند که به روزرسانی نرم افزار و میان افزار محصول مورد ارزیابی را به صورت دستی آغاز کند و [از سازوکار به روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به روزرسانی].	
۵۱	**به روزرسانی امن ۳**
محصول مورد ارزیابی باید در صورت استفاده از به روزرسانی به روش خودکار، پیش از نصب به روزرسانی های نرم افزاری و میان افزاری، با استفاده از [درهم ساز منتشرشده]، ابزاری را برای احراز هویت میان افزار آنها در اختیار محصول مورد ارزیابی قرار دهد.	

۷/۵ تخصیص منابع

شماره الزام	نام الزام
۵۲	**تحمل خطا ۱**
محصول باید از عملکرد [تمام کارکردهای اصلی] هنگام رویداد شکست های زیر اطمینان حاصل کند: [شکست نرم افزاری]	

۸/۵ کلاس دسترسی به محصول

شماره الزام	نام الزام
۵۳	**محدودیت بر روی چندین نشست همزمان ۱**
محصول باید حداکثر تعداد نشست های همزمان متعلق به یک کاربر را محدود کند.	
۵۴	**خاتمه دادن به نشست ها توسط محصول ۱**
محصول باید کلیه نشست های تعاملی راه دور[۵] را پس از مدت زمان [بازه زمانی که توسط مدیر تنظیم می شود] غیرفعال بودن، خاتمه دهد.	
۵۵	**خاتمه دادن به نشست ها توسط کاربر ۱**
محصول باید به کاربری که خود آغازگر نشست بوده است اجازه ی خاتمه نشست را بدهد.	
۵۶	**سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [روز، زمان] باشد.	
۵۷	**سوابق دسترسی به محصول ۲**
در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان] و تعداد تلاش ناموفق تا آخرین ایجاد نشست موفقیت آمیز باشد.	
۵۸	**سوابق دسترسی به محصول ۳**
محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک کند.	

[۵] Remote

۵۹	برقراری نشست ۱
محصول باید قادر به ممانعت از ایجاد نشست بر اساس [مکان] باشد.	

۹/۵ کلاس کانالهای/مسیرهای مورد اعتماد

برای این کلاس تعدادی الزام مبتنی بر انتخاب در « پیوست دو» ارائه شده است.

شماره الزام	نام الزام
۶۰	مسیر امن ۱
محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [HTTPS] مسیر ارتباطی امنی فراهم کند تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه دور 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 کند و تغییرات را تشخیص دهد.	
۶۱	مسیر امن ۲
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۶۲	مسیر امن ۳
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت های راه دور مدیر سیستم الزامی کند.	

۶ الزامات تضمین امنیت

اهداف امنیتی تعریف شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی شده در بخش ۴ در نظر گرفته شدهاند. الزامات کارکردی در بخش ۶ بیان رسمی و استانداردی از «اهداف امنیتی» است. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می باشند تا بر اساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل بر روی محصول انجام دهد.

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

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول را در اختیار آزمایشگاه قرار میدهد و محیط آزمون آن را فراهم می کند؛ و سپس فعالیت های تضمین که در سند هدف امنیتی مطرح شده، توسط آزمایشگاه انجام می شود. نتایج این فعالیت ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده سازی
Life cycle Support	ALC_CMC.1	برچسب گذاری محصول

نام کلاس	نام الزام	توضیحات
	ALC_CMS.1	پوشش پیکربندی محصول
Security Target	ASE_CCL.1	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه های توسعه یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.1	اهداف امنیتی
	ASE_REQ.1	الزامات امنیتی معین
	ASE_TSS.1	خلاصه مشخصات هدف ارزیابی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب پذیری

۱/۶ کلاس توسعه

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

مشخصات کارکردی:

مشخصات کارکردی، واسط های کارکرد امنیتی محصول را توصیف می کند اما نیازی به شرح مفصل و کاملی از این واسط ها نیست. فعالیت های این خانواده باید بر روی شناخت واسط های معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر:** مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.1D) **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.2D) **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند.

مؤلفه های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر:** مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.1C) **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[۶] و پشتیبان کننده ی الزام کارکرد امنیتی[۷] توصیف کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.2C) **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده ی الزام کارکرد امنیتی را مشخص کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.3C) **شرح مؤلفه:** مشخصات کارکردی باید برای دسته بندی ضمنی واسط های غیر مداخله کننده ی الزام کارکرد امنیتی دلایلی را ارائه کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.4C) **شرح مؤلفه:** ردیابی باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر:** مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه های محتوایی را برآورده می کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه:** (ADV_FSP.1.2E) شرح مؤلفه: ارزیاب باید مشخص کند که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس های «راهنما»، «آزمون» و «آسیب پذیری» ارائه شده است.

[۶] SFR-enforcing TSFI
[۷] SFR-supporting TSFI

۲/۶ 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 می تواند نقش خود را برای کارکرد امنیتی ایفا کند) ارائه می شود.

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 قابلیت های محصول، محیط عملیاتی یا هر دو است.

۶/۲/۱ راهنمای کاربردی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی (AGD_OPE)	**نام عنصر:** راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.1D) **شرح مؤلفه:** توسعه دهنده باید راهنمای کاربردی ارائه کند.

مؤلفه های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی (AGD_OPE)	**نام عنصر:** راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.1C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف کند، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.2C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسط های در دسترس ارائه شده توسط محصول به صورت امن استفاده می گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.3C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین کند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.4C)

مؤلفه های محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط کند، همانند تغییر مشخصات امنیتی موجودیت های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.5C) **شرح مؤلفه:** 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 ۱ **شماره مؤلفه:** (AGD_OPE.1.6C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می شوند توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.7C) **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه های اقدامات ارباب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی (AGD_OPE)	**نام عنصر:** راهنمای کاربردی ۱ **شماره مؤلفه:** (AGD_OPE.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه های محتوایی را برآورده می کند.

۶/۲/۲ راهنمای آماده سازی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده سازی (AGD_PRE)	**نام عنصر:** راهنمای آماده سازی **شماره مؤلفه:** (AGD_PRE.1.1D) **شرح مؤلفه:** توسعه دهنده باید محصول را همراه با سند آماده سازی ارائه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده سازی (AGD_PRE)	**نام عنصر:** راهنمای آماده سازی ۱ **شماره مؤلفه:** (AGD_PRE.1.1C) **شرح مؤلفه:** مستندات آماده سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده سازی ۱ **شماره مؤلفه:** (AGD_PRE.1.2C) **شرح مؤلفه:** مستندات آماده سازی باید تمام مراحل لازم برای نصب امن محصول و آماده سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای آماده سازی (AGD_PRE)	**نام عنصر:** راهنمای آماده سازی ۱ **شماره مؤلفه:** (AGD_PRE.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می کند.
	نام عنصر: راهنمای آماده سازی ۱ **شماره مؤلفه:** (AGD_PRE.1.2E) **شرح مؤلفه:** ارزیاب باید رویه های آماده سازی شرح داده شده در سند را بکار ببرد تا تائید کند، محصول می تواند به صورت امن برای عمل نمودن آماده شود.

۳/۶ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی هایی از چرخه حیات محدود می گردد 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.

۶/۳/۱ قابلیت های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه ای که توسط فروشنده ارائه شده، است (بدین معنی که جدا از 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 می تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر:** برچسبگذاری محصول ۱ **شماره مؤلفه:** (ALC_CMC.1.1D) **شرح مؤلفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر:** برچسب گذاری محصول ۱ **شماره مؤلفه:** (ALC_CMC.1.1C) **شرح مؤلفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر:** برچسب گذاری محصول ۱ **شماره مؤلفه:** (ALC_CMC.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می کند.

۶/۳/۲ حوزه پیکربندی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی (ALC_CMS)	**نام عنصر:** پوشش پیکربندی محصول ۱ **شماره مؤلفه:** (ALC_CMS.1.1D) **شرح مؤلفه:** ارزیاب باید لیست پیکربندی محصول را ارائه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی (ALC_CMS)	**نام عنصر:** پوشش پیکربندی محصول ۱ **شماره مؤلفه:** (ALC_CMS.1.1C) **شرح مؤلفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مؤلفه:** (ALC_CMS.1.1C)

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی کند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی (ALC_CMS)	**نام عنصر:** پوشش پیکربندی محصول ۱ **شماره مؤلفه:** (ALC_CMS.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می کند.

۴/۶ 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 انتخاب های درست صورت گرفته شده در آن، لازم است.

۶/۴/۱ ادعاهای انطباق

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق (ASE_CCL)	**نام عنصر:** ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.1D) **شرح مؤلفه:** توسعه دهنده باید یک ادعای انطباق تهیه کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.2D) **شرح مؤلفه:** توسعه دهنده باید ارتباط منطقی ادعای انطباق تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق (ASE_CCL)	**نام عنصر:** ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.1C) **شرح مؤلفه:** ادعای انطباق باید حاوی یک ادعای انطباق معیار مشترک باشد که نسخه ی معیار مشترک که سند هدف امنیتی و محصول ادعای انطباق با آن دارند را مشخص کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.2C) **شرح مؤلفه**: ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش ۲ انطباق یا توسعه معیار مشترک را توصیف کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.3C) **شرح مؤلفه:** ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش ۳ انطباق یا توسعه معیار مشترک را توصیف کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.4C) **شرح مؤلفه:** ادعای انطباق معیار مشترک باید با تعریف مؤلفه های توسعه یافته سازگار باشد.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.5C) **شرح مؤلفه:** ادعای انطباق معیار مشترک باید تمامی پروفایل های حفاظتی و بسته های الزامات امنیتی که ادعاهای انطباق سند هدف امنیتی آنها را بیان دارد را شناسایی کند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق (ASE_CCL)	**نام عنصر:** ادعاهای انطباق ۱ **شماره مؤلفه:** (ASE_CCL.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می سازد.

۶/۴/۲ تعریف مؤلفه های توسعه یافته

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه های توسعه یافته (ASE_ECD)	**نام عنصر:** تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.1D) **شرح مؤلفه:** توسعه دهنده باید یک اظهارنامه از الزامات امنیتی تهیه کند.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.2D) **شرح مؤلفه:** توسعه دهنده باید یک تعریف مؤلفه های توسعه یافته تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه های توسعه یافته (ASE_ECD)	**نام عنصر:** تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.1C) **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید تمامی الزامات امنیتی توسعه یافته را مشخص کند.
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.2C) **شرح مؤلفه:** تعریف مؤلفه های توسعه یافته باید یک مؤلفه توسعه یافته برای هر الزام امنیتی توسعه یافته تعریف کند
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.3C) **شرح مؤلفه:** تعریف مؤلفه های توسعه یافته باید توصیف کند که چگونه هر مؤلفه توسعه یافته به مؤلفه های معیار مشترک، خانوادهها و کلاس ها مرتبط می شود.
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.4C) **شرح مؤلفه:** تعریف مؤلفه های توسعه یافته باید از مؤلفه های معیار مشترک موجود، خانواده ها، کلاسها و متدولوژی به عنوان یک مدل برای ارائه، استفاده کند.
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.5C) **شرح مؤلفه:** مؤلفه های توسعه یافته باید شامل المان های هدفمند و قابل اندازه گیری باشد، طوری که انطباق و عدم انطباق با این المان ها، قابل اثبات باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه های توسعه یافته (ASE_ECD)	**نام عنصر:** تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده میسازد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	نام عنصر: تعریف مؤلفه های توسعه یافته ۱ **شماره مؤلفه:** (ASE_ECD.1.2E) **شرح مؤلفه:** ارزیاب باید تائید کند که هیچ مؤلفه ی توسعه یافته ای به وسیله مؤلفه های موجود، به صورت شفاف قابل بیان نیست.

۶/۴/۳ معرفی هدف امنیتی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی (ASE_INT)	**نام عنصر:** معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.1D) **شرح مؤلفه:** توسعه دهنده باید یک سند معرفی هدف امنیتی تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی (ASE_INT)	**نام عنصر:** معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.1C) **شرح مؤلفه:** سند معرفی هدف امنیتی باید شامل مرجع هدف امنیتی، مرجع محصول، توصیف محصول و مرور کلی محصول باشد.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.2C) **شرح مؤلفه:** مرجع سند هدف امنیتی باید هدف امنیت را به صورت منحصربه فرد مشخص کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.3C) **شرح مؤلفه:** مرجع محصول باید محصول را مشخص کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.4C) **شرح مؤلفه:** مرور کلی محصول باید نحوه استفاده و ویژگی های اصلی محصول را به صورت خلاصه بیان کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.5C) شرح مؤلفه: مرور کلی محصول باید نوع محصول را معرفی کند

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.6C) **شرح مؤلفه:** مرور کلی محصول باید هر سختافزار/نرم افزار/ثابتافزار غیر از محصول مورد ارزیابی را که بهوسیله محصول استفاده میشود معرفی کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.7C) **شرح مؤلفه:** شرح محصول باید حوزه فیزیکی محصول را توصیف کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.8C) **شرح مؤلفه:** شرح محصول باید حوزه منطقی محصول را توصیف کند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی (ASE_INT)	**نام عنصر:** معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می سازد.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه:** (ASE_INT.1.2E) **شرح مؤلفه:** ارزیاب باید تائید کند که مرور کلی محصول، مرجع محصول و خلاصه محصول با یکدیگر سازگار هستند.

۶/۴/۴ اهداف امنیتی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی (ASE_OBJ)	**نام عنصر:** اهداف امنیتی ۱ **شماره مؤلفه:** (ASE_OBJ.1.1D) **شرح مؤلفه:** توسعه دهنده باید که اظهارنامه از اهداف امنیتی تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی (ASE_OBJ)	**نام عنصر:** اهداف امنیتی ۱ **شماره مؤلفه:** (ASE_OBJ.1.1C) **شرح مؤلفه:** اظهارنامه اهداف امنیتی باید اهداف امنیتی برای محیط عملیاتی را توصیف کند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی (ASE_OBJ)	**نام عنصر:** اهداف امنیتی ۱ **شماره مؤلفه:** (ASE_OBJ.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می سازد.

۶/۴/۵ الزامات امنیتی معین

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین (ASE_REQ)	**نام عنصر:** الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.1D) **شرح مؤلفه:** توسعه دهنده باید که اظهارنامه از اهداف امنیتی تهیه کند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.2D) **شرح مؤلفه:** توسعه دهنده باید ارتباط منطقی بین الزامات را تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین (ASE_REQ)	**نام عنصر:** الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.1C) **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید الزامات کارکردی و تضمین امنیت را توصیف کند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.2C) **شرح مؤلفه:** تمامی موجودیت های فعال، غیرفعال، عملیات، مشخصه های امنیتی، موجودیت های خارجی و دیگر اصطلاحاتی که در الزامات کارکردی و تضمین امنیت استفاده می شوند، باید توصیف گردند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.3C) **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید تمامی عملیات بر روی الزامات امنیتی را معرفی کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.4C) **شرح مؤلفه:** تمامی عملیات باید به درستی انجام گیرند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.5C) **شرح مؤلفه:** هر وابستگی بین الزامات امنیتی باید ارضاء گردد، یا ارتباط منطقی الزامات امنیتی نشان دهد که نیاز به ارضاء نیست.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.6C) **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید سازگاری داخلی داشته باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی (ASE_REQ)	**نام عنصر:** الزامات امنیتی معین ۱ **شماره مؤلفه:** (ASE_REQ.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می سازد.

۶/۴/۶ خلاصه مشخصات هدف ارزیابی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی (ASE_TSS)	**نام عنصر:** خلاصه مشخصات هدف ارزیابی ۱ **شماره مؤلفه:** (ASE_TSS.1.1D) **شرح مؤلفه:** توسعه دهنده باید یک سند خلاصه مشخصات محصول تهیه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
خلاصه مشخصات هدف ارزیابی (ASE_TSS)	**نام عنصر:** خلاصه مشخصات هدف ارزیابی ۱ **شماره مؤلفه:** (ASE_TSS.1.1C) **شرح مؤلفه:** سند خلاصه مشخصات محصول باید تشریح کند که چگونه محصول الزامات کارکردی امنیت را برآورده می کند.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی (ASE_TSS)	**نام عنصر:** خلاصه مشخصات هدف ارزیابی ۱ **شماره مؤلفه:** (ASE_TSS.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می سازد.
	نام عنصر: خلاصه مشخصات هدف ارزیابی ۱ **شماره مؤلفه:** (ASE_TSS.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که خلاصه مشخصات محصول با مرور کلی محصول و خلاصه محصول سازگار است

۵/۶ کلاس آزمون

آزمون محصول برای بررسی بخش های کارکردی سیستم و همچنین بخش هایی که طراحی و پیاده سازی آنها برای سیستم دارای آسیبهای امنیتی است، در نظر گرفته میشود. آزمون بخش های کارکردی سیستم از طریق خانواده ATE_IND ؛ و آزمون بخشهایی که طراحی و پیاده سازی آسیب زایی دارند از طریق خانواده AVA_VAN صورت میگیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته شده و واسط هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می گیرد، انجام می گردد. نتایج آزمون و تحلیل آسیب پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۶/۵/۱ آزمون مستقل

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

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	**نام عنصر:** آزمون مستقل ۱ **شماره مؤلفه:** (ATE_IND.1.1D) **شرح مؤلفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	**نام عنصر:** آزمون مستقل ۱ **شماره مؤلفه:** (ATE_IND.1.1C) **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	**نام عنصر:** آزمون مستقل ۱ **شماره مؤلفه:** (ATE_IND.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، مؤلفه های محتوایی را برآورده می کند.
	نام عنصر: آزمون مستقل ۱ **شماره مؤلفه:** (ATE_IND.1.2E) **شرح مؤلفه:** ارزیاب باید زیرمجموعه ای از توابع امنیتی محصول را آزمون کند تا تائید شود که توابع امنیتی محصول به صورت مشخص شده عمل می کنند.

۶/۶ کلاس آسیب پذیری

این کلاس به پوشش آسیب پذیری های قابل بهره برداری که در توسعه و عملیات محصول ممکن است وجود داشته باشد می پردازد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	نام عنصر: آسیب پذیری ۱ شماره مؤلفه: (AVA_VAN.1.1D) شرح مؤلفه: توسعه دهنده باید برای آزمودن، محصول را ارائه کند.

مؤلفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	**نام عنصر:** آسیب پذیری ۱ **شماره مؤلفه:** (AVA_VAN.1.1C) **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب پذیری (AVA_VAN)	**نام عنصر:** آسیب پذیری ۱ **شماره مؤلفه:** (AVA_VAN.1.1E) **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه های محتوایی را برآورده می کند..
	نام عنصر: آسیب پذیری ۱ **شماره مؤلفه:** (AVA_VAN.1.2E) **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب پذیری های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
	نام عنصر: آسیب پذیری ۱ **شماره مؤلفه:** (AVA_VAN.1.3E) **شرح مؤلفه:** ارزیاب باید بر اساس آسیب پذیری های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت میگیرند، مشخص کند.

۷ خلاصه مشخصات محصول

نسخه ۱/۰ سند هدف امنیتی سامانه سرویا / وندیا نسخه ۱/۱۰ توسط واحد راهکار و محصول و واحد فنی گروه فناوری پرند تدوین شده است و رعایت الزامات کارکرد امنیتی ذیل در آن ادعا شده است:

- محصول هر یک از رویداد های امنیتی را با فیلدهای ذیل نگهداری می کند و بر اساس کلیه مقادیر اعلام شده امکان جستجو و فیلتر کردن را دارا می باشد. حذف رکوردها تنها در صورت دسترسی غیرمجاز به پایگاه داده امکان پذیر است:
  - نوع کلاینت
  - تاریخ و زمان ایجاد
  - محتوای رویداد
  - نوع رویداد
  - آدرس آی پی
  - شناسه کاربری
- مقادیر مجاز برای نوع کلاینت در محصول عبارتند از:
  - پورتال کاربران (WSSP)
  - پورتال کارشناسان (PTW)
  - نرم افزار کلاینت (Clickonce)
- مقادیر مجاز نوع رویداد عبارت است از:
  - ورود ناموفق Domain
  - ورود ناموفق Forms
  - ورود ناموفق Identity Service
  - ورود ناموفق Shibboleth
  - ورود ناموفق Normal
  - ورود ناموفق Client
  - ورود موفق Domain
  - ورود موفق Forms
  - ورود موفق Identity Service
  - ورود موفق Shibboleth
  - ورود موفق Normal
  - ورود موفق Client

- قفل کاربر Domain
- قفل کاربر Forms
- قفل کاربر Identity Service
- قفل کاربر Shibboleth
- قفل کاربر Normal
- قفل کاربر Client
- خروج عادی
- خروج به علت تغییر دسترسی کاربر
- خروج به علت تغییر دسترسی کارشناس
- دریافت فایل
- بارگذاری فایل
- تغییر پروفایل کاربر
- تغییر پروفایل کارشناس
- افزودن نقش دسترسی
- حذف نقش دسترسی
- تغییر نقش دسترسی
- تغییر پارامترهای شرکت
- ورود همزمان
- ورود غیر مجاز
- دسترسی غیر مجاز
- مشاهده لاگ امنیت

- محتوای لاگ های خاص به شرح ذیل می باشد:
  - افزودن نقش دسترسی: Save Role (شناسه نقش)
  - حذف نقش دسترسی: Delete Role (شناسه نقش)
  - تغییر نقش دسترسی: ObjectPK (کلید اصلی شیء) ; SubjectPK (کلید اصلی نقش) ; Rights (کلید حقوق دسترسی مرتبط)
  - تغییر پارامترهای شرکت: (عنوان پارامتر شرکت) value changed from (مقدار قدیم) to (مقدار جدید)
- محصول در صورت طولانی شدن داده های ممیزی، از طریق پیام سیستمی نسبت به انجام اطلاع رسانی های لازم اقدام می نماید.
- محصول برای وارسی صحت داده های ممیزی و داده های رکورد بر اساس یک الگوریتم رمزنگاری مشخص GCM و اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیت اجرا می شود که مطابق با NIST SP 800-38D می باشد. همچنین برای تولید داده درهم سازی بر اساس مجموعه الگوریتم های رمزنگاری مشخص SHA-256 و SHA-384 و اندازه کلید رمزنگاری ۲۵۶ و ۳۸۴ بیت استفاده می شود که مطابق با ISO/IEC 10118-3:2004 می باشد.
- محصول با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم، تعداد تلاش های احراز هویت ناموفق را مدیریت می نماید.
- محصول می تواند احراز هویت را از طریق نام کاربری و رمز عبور و یا Active Directory انجام دهد.

- محصول زمانی که یک نشست جدید قرار می شود، اطلاعات موجود از نشست های قبلی را حذف می نماید و رکورد ممیزی مربوطه ثبت می گردد.
- محصول می تواند بر روی نوع فایل ها، تعداد فایل ها، محتوای فایل ها بر اساس نوع کنترل های لازم را انجام دهد.
- محصول می تواند هنگام تشخیص خطای صحت داده ممیزی مربوطه را ثبت نماید.
- محصول می تواند دسترسی بر اساس نوع کاربری که بر اساس نقش های کاربر مشخص می شود را بر روی عملیات های متفاوت اعمال نماید.
- محصول می تواند سطح دسترسی را با توجه به هویت کاربر، نقش ها و مجوزهای کاربر مجاز و اطلاعات نشست کاربر، بر روی موجودیت های غیرفعال اعمال نماید. این موضوع در محصول با عنوان محرمانگی داده مورد استفاده قرار می گیرد.
- محصول دارای قابلیت محدودسازی توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر می باشد.
- محصول می تواند با اعمال تعیین سطح دسترسی بر اساس نقش، توانایی تغییر پیش فرض، پرس و جو، تغییر، حذف و ایجاد مشخصه های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود نموده و امکان در نظر گرفتن مقادیر پیش فرض محدود شده محصول برای مشخص های امنیتی که برای اعمال خط مشی استفاده می شوند، وجود داشته و مدیریت سیستم از طریق پیکربندی می تواند هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش فرض را لغو و تغییر دهد.
- محصول می تواند توانایی تغیر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم و توانایی تغییر پیش فرض، پرس و جو، تغییر رمز عبور و ... را به کاربر عادی محدود نماید.
- محصول قابلیت تعریف نقش های متفاوت بر اساس نیازمندی های فرآیند را دارا می باشد.
- محصول می تواند کاربران را با نقش های مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیرفعال تحت کنترل خود را به مدیر سیستم محدود کند.
- محصول در صورت رخ دادن هر گونه شکستی، کاربر عادی خطای عمومی را مشاهده می کند و مدیر سیستم می تواند جزئیات پیام را مشاهده کند.
- محصول می تواند هنگام انتقال داده ها بین بخش های مجزای خود، از آنها در برابر افشاء یا تغییر محافظت نماید.
- محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می باشد.
- محصول می تواند کلیه نشست های راه دور را پس از مدت زمان قابل تنظیم، خاتمه دهد.
- محصول می تواند در صورت برقراری نشست موفقیت آمیز، نسبت به نمایش آخرین تلاش موفق یا ناموفق، اقدام نماید.
- محصول می تواند مسیر ارتباطی امن را با استفاده از پروتکل HTTP میان خود و موجودیت IT معتبر همچون کاربر سامانه را فراهم نماید.