به نام خدا

سند هدف امنیت
سامانه جامع اطلاعات پژوهشی
(پژوهان) نسخه 1.0

شرکت بهینه سازان نرم افزار بهسان ایساتیس

تابستان-1403
نسخه 1.0

فهرست

شرکت بهینه سازان نرم افزار بهسان ایساتیس

1 معرفی

مدیریت محصولات پژوهشی اعم از طرح، کتاب، مقاله و ... به نحوی که هم یک بانک جامع از تولیدات پژوهشی سازمان در سامانه تجمیع می شود و هم فرایند گردش کار تولیدات پژوهشی از ابتدا تا انتها توسط سامانه انجام می پذیرد و در انتها گزارش های مد نظر از سامانه استخراج می شود. در طی فرآیند ذینفعان مختلف اعم از پژوهشگران، کارشناسان و مدیران سازمان و همچنین سازمان های همکار می توانند به سامانه متصل شده و در جریان ریز فرآیندها قرار بگیرند. همچنین در طول فرآیند پیام داخلی، ایمیل و پیامک برای ذینفعان ارسال می گردد.

1.1 مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه اطلاعات پژوهشی(پژوهان)
نسخه	1.0
تاریخ	1403.05.05
نویسندگان	سهراب یوسفی نازکی

نام شرکت	بهینه سازان نرم افزار بهسان ایساتیس
نام محصول	سامانه اطلاعات پژوهشی (پژوهان)
نوع محصول	برنامه کاربردی تحت وب
نسخه‌ی محصول	15.0.0

حداقل نیازمندی نرم‌افزاری/سخت‌افزاری/میان‌افزاری محصول

شرکت بهینه سازان نرم افزار بهسان ایساتیس

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

سخت‌افزار /نرم‌افزار /میان‌افزار	حداقل الزامات
سیستم عامل سرور	Microsft Windows 2016 Standard Edition, Windows 2019 Standard Edition
سرور وب	Weblogic 14.1.1.0
JDK	JDK8u410+
مرورگر کلاینت	Firefox, Chrome
سرور پایگاه داده	HDD:500GB+, Ram:12GB,CPU:4Cores
سرور وب	HDD:100GB+, Ram:8GB,CPU:4Cores

2 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 1.2 از سند «راهنمای نوشتن سند هدف امنیتی» مراجعه شود.

1.2 انطباق با استاندارد ارزیابی امنیتی معیار مشترک

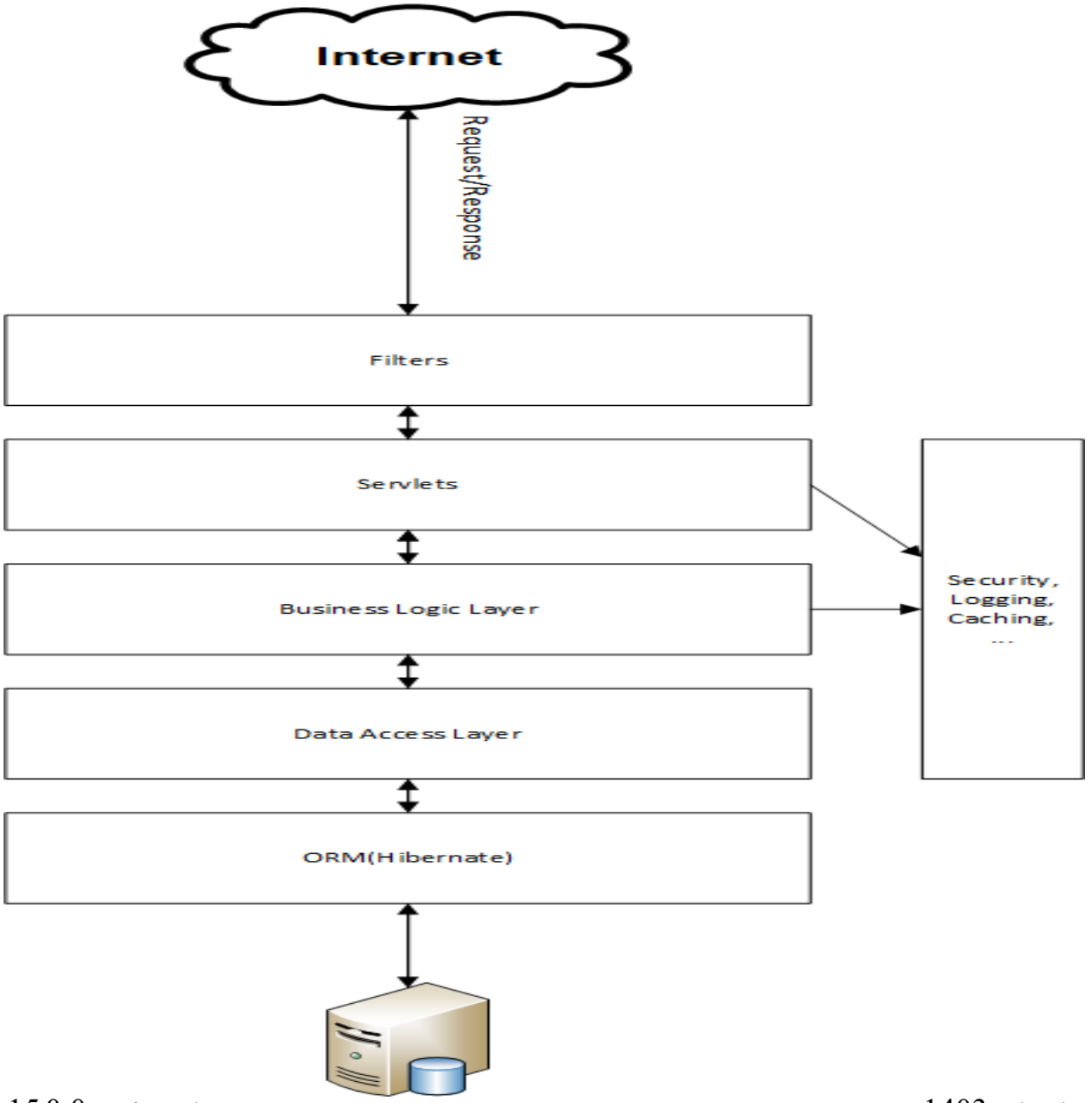
انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
نام پروفایل حفاظتی	پروفایل حفاظتی برنامه های کاربردی تحت شبکه
سطح تضمین امنیتی	EAL1

2.2 شرح محصول

نرم افزار از بخش های مختلف تشکیل شده است که هر قسمت بطور کلی یک لایه دریافت درخواست ها و برگرداندن پاسخ ها را دارد و یک لایه وظیفه بیزینس یا منطق را بر عهده دارد و یک لایه هم وظیفه ارتباط با پایگاه داده را بر عهده دارد. لایه بیزینس رابط بین دو لایه دیگر هست و دو لایه دیگر ارتباط مستقیم باهم ندارند. همچنین چنانچه بخش های مختلف بخواهند با هم ارتباط برقرار نمایند لایه بیزینس یکدیگر را فراخوانی می نمایند(بعضی از بخش ها ممکن است هر سه لایه را نداشته باشند).

به موازات لایه های گفته شده برای بخش های مختلف یکسری امکانات سراسری هم وجود دارند که در عموما در دولایه اول مورد استفاده قرار می گیرند مانند امکانات مربوط به امنیت و ثبت و مدیریت لاگ ها.

برای ارتباط با پایگاه داده از Hibernate به عنوان ORM استفاده شده است.

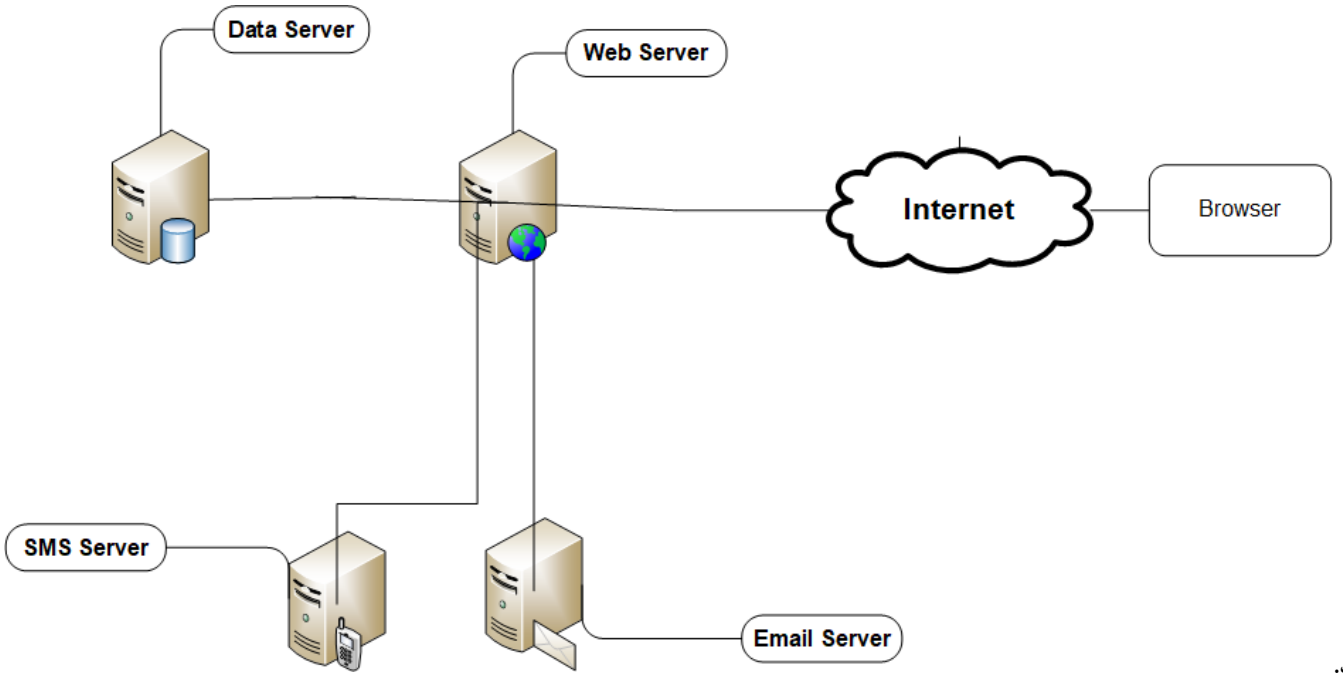

Internet
Request/Response
Filters
Servlets
Business Logic Layer
Data Access Layer
ORM(Hibernate)
Security,
Logging,
Caching,
...

1.2.2حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
مدل و نسخه سیستم‌عامل	Windows Server 2016 Standard, Windows Server 2019 Standard
مدل و نسخه وب‌سرور	Weblogic 14.1.1.0
مدل و نسخه پایگاه داده	MS SQL Server 2019+
زبان برنامه‌نویسی	Java

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.

2.2.2حوزه منطقی

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

کارکردها	توصیف
احراز هویت با نام کاربری و کلمه عبور	*امکان تعیین نام کاربری و کلمه عبور با خط مشی های امنیتی تعیین شده در هنگام ثبت نام کاربر وجود دارد و پس از تایید و فعال سازی کاربر توسط مدیران سامانه، کاربر می تواند با نام کاربری و کلمه عبور تعیین شده وارد سامانه شود.*
احراز هویت با رمز یکبار مصرف	*در صورت درخواست کاربر، یک کلمه عبور تصادفی یکبار مصرف با زمان اعتبار محدودبرای شماره همراه از پیش ذخیره شده کاربر پیامک می گردد.*

شکل 1: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

بازیابی کلمه عبور از طریق ایمیل	*در صورت فراموشی کلمه عبور، یک ایمیل برای ایمیل از پیش ذخیره شده کاربر ارسال و امکان تعیین کلمه عبور جدید توسط کاربر وجود خواهد داشت.*
رویدادنگاری	*تمامی فعالیت های کابران ثبت و امکان جستجو و مشاهده فعالیت ها توسط مدیران سامانه وجود دارد.*
کنترل دسترسی	*بر اساس دسترسی های تعیین شده برای کاربر در سه سطح درختواره سازمانی، دسترسی به سامانه و همچنین دسترسی نقش های کاربر در مراحل مختلف گردش کار، کاربر می تواند به داده ها و مولفه های سامانه پس از احراز هویت دسترسی داشته باشد.*

3 مسائل امنیتی

1.3 تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا کند. این دسترسی میتواند با استفاده هویت سرقتی، آدرسIPجعلی و غیره صورت گیرد. مهاجم میتواند با سود بردن از نقض های 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 پیداکند. همچنین مهاجم میتواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده کهدر طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده های میتوانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به داده ها و خود محصول سبب آسیب شود.

تهدیدات	توضیحات
تغییر غیرمجاز	رکوردهای، مستندات و داده های حفاظت شده توسط محصول میتواند بدون مجوز تغییر یابند.مهاجم میتواند با گمراه نمودن مدیر سیستم،واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم میتواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها و مستندات تضمین شده نیست. مهاجم ممکن است درصددتغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیداکند.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول میتواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول است تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می تواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم میتواند با اضافه کردن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه کند.
افشای اطلاعات	داده های محرمانه که توسط محصول محافظت میشوند 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 اپراتورواردکننده داده میتواند 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 می گیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده ای از حمله شامل ارسال درخواستهای بسیار از یک رنج IP مشخص است که به نام حمله DoS شناخته می شود. نوع دیگر پیشرفته تر حملهDDoS است که ازBOTNET استفاده می کند و محدودیتی بر روی آدرسIP ورودی ندارد.

تهدیدات	توضیحات
دادههای ورودی مخرب	مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول واردکند. با استفاده از این تهدید، مهاجم می تواند به داده کاربر خاص دسترسی پیداکند، 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 بالاتر کند.
شنود شبکه	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر میشود تا انتقال داده های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده های رد و بدل 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.

2.3 خط‌مشی امنیتی

خط مشی ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولا به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار میگیرند.
پیکربندی مناسب	پیکربندی پیش فرض محصول ومؤلفه 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

خط مشی ها	توضیحات
	و صفحات 404 ، 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 به طور گسترده مورد استفاده قرار می گیرد؛ بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می توان 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.

3.3 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 الزم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ می نمایند.
محیط امن	فرض شده است که تمام پیش بینی 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

فرضیات	توضیحات
	و مستندات که غیرقانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت میگیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و 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 الزم 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 الزم در قبال حملات DDoS اتخاذ می شود.

4 اهداف امنیتی

1.4 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 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 وآنها را به طور امن احراز هویت کند و مطابق با نقش و مجوزهایشان مجازکند. محصول باید برای احراز هویت کاربر، قوانینی تعریف کند طوری که کاربران را ملزم به استفاده ازکلمه 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 ساز و کارهای قویتری مدیر سیستم را احراز هویت کند. از جمله سازوکارها میتوان به محدود نمودن رنجIP، محدود نمودن بازه زمانی، احرازهویت بر اساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش ها اشاره نمود.

هدف امنیتی	توضیحات
کنترل جریان داده	محصول بایدگردش داده های غیرمجاز را کنترل و مدیریت کند. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست ها از یک رنج IP تعریف شده می تواند بیانگر حمله DoS 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 ساز و کارهای 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 وکارآمد سیستم فراهم کند. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط های 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 سریعا 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 دادههای باقیمانده	محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می گردد.

هدف امنیتی	توضیحات
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

2.4 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 DoSیا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی میتوان به غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده ی محصول در زمینه امنیت تجربه داشته وآنها اقدامات مقابله ای لازم برای تمام آسیب پذیری های امنیتی شناخته شده رادر نظر می گیرد.

هدف امنیتی	توضیحات
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه های غیر از محصول نیز مورد ممیزی قرار می گیرند. 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 یاغیرقابل دسترس گردند.
پشتیبان گیری مناسب	نسخه پشتیبان بایدایجاد گردیده و برای یک بازه زمانی منطقی تمام داده های باقیمانده در محیط عملیاتی محصول را حفظ کند. برای این منظور ممکن است ازروال های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مؤلفه های سخت افزاری نیز نسخه پشتیبان تهیه گردد.

5 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
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 احرازهویت ناموفق ۱**	FIA_AFL.1.1
۳۰	**مدیریت احرازهویت ناموفق ۲**	FIA_AFL.1.2
۳۱	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۳۲	**مدیریت کلمه عبور**	FIA_PMG_EXT.1.1
۳۳	**احرازهویت کاربر ۱**	FIA_UAU.1.1
۳۴	**احرازهویت کاربر ۲**	FIA_UAU.1.2
۳۵	**سازوکار احرازهویت چندگانه ۱**	FIA_UAU.5.1
۳۶	**سازوکار احرازهویت 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 مشخصههای امنیتی کاربر با موجودیت فعال متناظر ۳**	FIA_USB.1.3
۴۰	**مدیریت کارکرد در محصول ۱**	FMT_MOF.1.1
۴۱	**مدیریت مشخصههای 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	**نقشهای امنیتی ۱**	FMT_SMR.1.1
۴۵	**نقشهای 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	**بهروزرسانی امن ۲**	FPT_TUD_EXT.1.2
۵۱	**بهروزرسانی 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 نشستها توسط محصول ۱**	FTA_SSL.3.1
۵۵	**خاتمه دادن به نشستها 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
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.)3(1
۶۶	**عملیات رمزنگاری ۱ (۴)**	FCS_COP.)4(1.1
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/ احرازهویت (۴)**	FCS_TLSS_EXT.2.4
۷۸	**الزامات پروتکل TLS Server/ احرازهویت (۵)**	FCS_TLSS_EXT.2.5
۷۹	**الزامات پروتکل TLS Server/ احرازهویت (۶)**	FCS_TLSS_EXT.2.6
۸۰	**الزامات پروتکل (۱) X509/ ابطال**	FIA_X509_EXT.1.1/Rev
۸۱	**الزامات پروتکل (۲) X509/ ابطال**	FIA_X509_EXT.1.2/Rev

۸۲	**الزامات پروتکل (۳) X509**	FIA_X509_EXT.2.1

1.5 ممیزی امنیت (Log)

در این رده توانایی‌های محصول از نظر امکان تولید داده ممیزی (Log) مناسب برای فعالیت‌های مختلفی که در محصول صورت می‌گیرد، در شرایط مختلف سنجیده می‌شود.

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
1	**محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[1] تولید کند (Log ثبت نماید).**			☑	
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	☑		
		تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	☑		
		عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	☑		

[1] Log

		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	☑		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	☑		
		تمام کاربردهای سازوکار احراز هویت	☑		
		نتایج نهایی عملیات احراز هویت	☑		
		تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	☑		
		شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	☑		
		تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	☑		
		تمامی درخواست‌ها (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	☑		
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	☑		
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑		
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑		
		استفاده از کارکردهای مدیریتی	☑		
		تغییرات در گروه کاربران	☑		
		شکست در کارکردهای امنیتی محصول	☑		

		تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	☑		
		تلاش موفق یا ناموفق برای برقراری نشست.	☑		
		ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	☑		
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	☑		
		خاتمه به نشست غیرفعال توسط مدیر سیستم	☐		
		سایر موارد	☐		
2	**محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.**			☑	
	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	تاریخ و زمان رویداد	☑		
		نوع رویداد	☑		
		هویت ایجادکننده رویداد	☑		
		نتیجه رویداد	☑		
		آدرس IP ایجادکننده رویداد	☑		
		سایر موارد	☐		
3	**محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.**			☑	

4	**ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			☑	
	موارد ی که در ثبت‌نشان‌ها وجود دارند، مشخص شوند.	نبود داده نامفهوم در رکوردها	☑		
		نبود بخش‌های نامرتبط	☑		
		وجود داده معتبر و مناسب در هر بخش	☑		
5	**محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			☑	
	موارد ی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	هویت موجودیت فعال	☑		
		نوع حساب کاربری	☐		
		تاریخ/زمان	☑		
		روش اتصال کاربر	☐		
		نوع رخداد	☑		
		مکان رویداد	☑		
		سایر موارد	☐		
6	**محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.**			☑	
	روش های تشخیص مشخص شود. (وجود یک	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	☐		
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☐		
		فقط خواندنی کردن ثبت‌نشان‌ها در محصول	☑		

	مورد لازم و کافی است)	سایر موارد	☐		
7	**محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**		☑		
	روش‌های اطلاع‌رسانی مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐		
		ارسال پیام	☐		
		از طریق واسط کاربر مجاز	☑		
		سایر موارد	☐		
8	**محصول باید توانایی تولید ثبت‌نشان (ثبت Log) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.**		☑		
	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن ثبت‌نشان‌ها	☐		
		ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☐		
		بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده	☐		
		سایر موارد	☑		در صورت عبور حجم ثبت نشان ها از آستانه تعریف شده و وجود کمتراز یکصد کیلوبایت فضای خالی در جدول ثبت نشان ها، امکان ورود به سامانه مسدود خواهد شد و هیچ کاربری نمی تواند وارد حساب کاربری خود شود.

2.5 رمزنگاری

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری واحدهای[۲] رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده، از رمزنگاری استفاده می‌شود و این رمزنگاری‌ها می‌توانند به صورت متقارن و نامتقارن صورت گیرد. در رمزنگاری متقارن، از یک کلید مشترک برای رمزگذاری و رمزگشایی استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یک زوج کلید (کلید عمومی و کلید خصوص) صورت می‌گیرد. الگوریتم‌ها می‌توانند با طول کلیدهای مختلف و روش‌های مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این رده، توانایی محصول از این جهت مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین الگوریتم‌های درهم‌سازی (Hash) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	رده رمزنگاری				توضیحات
1	**محصول باید قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			☑	
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد	مد عملیاتی CBC و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38A)	☐		
		مد عملیاتی GCM و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38D)	☑		طول کلید 128 و 256 بیتی
		مد عملیاتی CTR و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در ISO10116)	☐		

[2] Modules

	لازم و کافی است.)				
2	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**		☑		
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	الگوریتم SHA-1 با اندازه خلاصه پیام 160 بیت	☐		
		الگوریتم SHA-256 با اندازه خلاصه پیام 256 بیت	☑		
		الگوریتم SHA-384 با اندازه خلاصه پیام 384 بیت	☑		
		الگوریتم SHA-512 با اندازه خلاصه پیام 512 بیت	☐		
3	**در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)**		☑		
	روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☑		
		سایر موارد	☐		

4	**در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☑	
	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری 2048 بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش 5.5، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال 2 و یا الگوی امضای دیجیتال 3)	☑		
		الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری 256 بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش 6.4، استاندارد امضای دیجیتال (DSS) بخش 6 و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☑		

3.5 شناسایی و احراز هویت

در این رده توانایی‌های محصول از نظر امکان شناسایی و احراز هویت کاربر در حالت‌های مختلف و اقدامات متقابل در راستای عدم برقراری آنها، بررسی می‌گردد.

شماره الزام	رده شناسایی و احراز هویت				توضیحات
1	**محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.**	☑			
	مقدار یا یازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	☑	یک عدد مثبت ثابت		5 مرتبه
		☐	یک عدد مثبت قابل تنظیم توسط مدیر		
2	**محصول باید هنگامی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.**	☑			

	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.) لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	☐		
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	☑		20 ثانیه
		استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)	☑		کپچا
		سایر موارد	☐		

3	**محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.**			☑	
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	☑		
		روش احراز هویت مورد استفاده	☑		
		داده احراز هویت	☑		
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	☑		
		نقش کاربر	☑		
		سایر موارد	☐		
4	**محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.**			☑	
	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	استفاده از حروف کوچک	☑		
		استفاده از حروف بزرگ	☑		
		استفاده از اعداد	☑		
		استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...)	☑		
		حداقل طول 8 یا بیشتر (قابل تنظیم)	☑		
		سایر موارد	☐		
5	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**			☑	

	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام دهد، انتخاب شود.	مشاهده راهنمای نحوه ورود به سیستم	☐		
		بازیابی گذرواژه	☑		
		هیچ اقدامی	☐		
		سایر موارد	☑		تماس با ما، اخبار پژوهشی،جستجوی طرح های تحقیقاتی و ...
6	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).**			☑	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و گذرواژه	☑		
		امضای دیجیتال	☐		
		سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	☐		
		OTP یا توکن	☑		
		احراز هویت دو فاکتوری	☐		
		سایر موارد	☐		
7	**محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.**			☑	
	ویژگی‌های امنیتی که محصول برای هر	شناسه کاربر	☑		
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	☑		

	کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	جزئیات واسط کلاینت	☐		
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☑		
		سایر موارد	☐		
8	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**			☑	
	در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشست‌های قبلی هنگام برقراری یک نشست جدید (به جز مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود.)	☑		
		بروزرسانی اطلاعات پیشینه احراز هویت	☑		
		سایر موارد	☐		

9	**محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			☑	
	قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑		
		سایر موارد	☐		

4.5 حفاظت از داده کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالک آن است. توضیح کامل داده کاربری در سند «*راهنمای سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه*» در قسمت اصطلاحات بیان گردیده است. در این رده، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

شماره الزام	رده حفاظت از داده‌ی کاربری				توضیحات
1	**محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر عادی	☑		
		سایر موارد	☐		
	موجودیت‌های غیرفعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها	سوابق، مستندات و فراداده	☑		
		داده متعلق به کاربران	☑		
		داده احراز هویت	☑		
		سایر موارد	☐		

	اعمال می‌شوند، مشخص گردد.				
	عملیاتی که خط‌مشی‌های کنترل دسترسی در رابطه با آنها اعمال می‌شوند، مشخص گردد.	ایجاد موجودیت غیرفعال جدید	☑		
		حذف موجودیت غیرفعال	☑		
		تغییر دسترسی‌ها به موجودیت غیرفعال	☑		
		عملیات بر روی فراداده وابسته به موجودیت غیرفعال	☑		
		سایر موارد	☐		
2	**محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**		☑		
	ویژگی‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	☑		
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	☑		
		سایر موارد	☐		
3	**محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در فهرست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.)**		☑		

4	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			☑	
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	☑		
		سایر موارد	☐		
5	**محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.**			☑	
6	**محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	ویژگی‌های امنیتی مرتبط با داده کاربری که	نوع داده	☑		
		حجم و اندازه	☑		حداکثر حجم 5242880 بیت

	در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	فرمت	☑		zip,rar,jpeg,txt,pdf,xlsx,xls,docx,doc,png,jpg,gif
		تعداد دفعات Import	☐		
		سایر موارد	☐		
7	**محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.**			☑	
8	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی را اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
		نوع داده	☑		

	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	حجم و اندازه	☑		از آنجایی که امکان دانلود فایل های آپلود شده وجود دارد، میزان حجم همان 5242880 بیت می باشد.
		فرمت	☑		zip,rar,jpeg,txt,pdf,xlsx,xls,docx,doc,png,jpg,gif
		سایر موارد	☐		
9	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**		☑		
	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☑		
		سایر موارد	☐		
10	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.**		☑		
	چگونگی تشخیص تغییر در داده‌های	مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	☑		
		سایر موارد	☐		

	کاربری حساس، مشخص شود.				
11	**محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.**			☑	
	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یک مورد لازم و کافی است)	ایجاد هشدار/اخطار برای نقش‌های مجاز	☑		
		تصحیح داده بر اساس مقادیر قبل	☐		
		سایر موارد	☐		

5.5 مدیریت امنیت

در این رده توانایی‌های محصول در مدیریت (حذف، تغییر، فعال کردن و ...) کارکردهای امنیتی (جمع‌آوری داده‌های سیستم، پیکربندی‌ها و ...) مورد بررسی قرار می‌گیرد. همچنین توانایی محصول در مدیریت نقش‌ها و دسترسی آنها برای اعمال مدیریت بر روی کارکردهای امنیتی سنجیده می‌شود.

شماره الزام	رده مدیریت امنیت				توضیحات
1	**محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.**			☑	
	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	تعیین و تغییر رفتار	☑		
		غیرفعال نمودن	☑		
		فعال نمودن	☑		
		سایر موارد	☐		
2	**محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام 7 از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
		پرس‌وجو	☑		

	عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	تغییر	☑		
		حذف	☑		
		تغییر پیش‌فرض	☐		
		سایر موارد	☐		
3	**محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.	تغییر پیش‌فرض	☐		
		حذف نمودن	☑		
		پرس‌وجو	☑		
		مقداردهی	☑		
		ایجاد	☑		
		مشاهده	☑		
		سایر موارد	☐		
4	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			☑	
	در صورتی که هرکدام از موارد مطرح‌شده،	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	☑		
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	☑		

	توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	☑ پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها			
		☑ مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول			
		☐ انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)			به عهده سیستم عامل است.
		☑ ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول			
		☑ در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.			
		☑ 1. مدیریت حد آستانه برای تلاش‌های ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.			
		☑ مدیریت معیارها برای تنظیم گذرواژه‌ها			
		☑ 1. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه 2. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.			
		☑ 1. مدیریت سازوکارهای احراز هویت			

		2. مدیریت قوانین مرتبط با احراز هویت			
		مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.	☑		
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	☑		
		مدیریت نقش‌ها در محصول	☑		
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	☑		
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑		
		1. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. 2. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	☑		
5	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**			☑	
	نقش‌هایی که در محصول پشتیبانی	مدیر سیستم	☑		
		کاربر پیشرفته	☑		
		کاربر عادی	☑		
		سایر موارد	☑		

	می‌شوند، مشخص گردد.			
6	**محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.**		☑	

6.5 حفاظت از توابع امنیتی محصول

در این رده، توانایی محصول در حفظ وضعیت امن در زمان رخ دادن شکست و همچنین حفاظت از داده‌ها هنگام تبادل بین اجزای محصول یا تبادل با موجودیت‌های دیگر، مورد بررسی قرار گرفته است.

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
1	**محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.**			☑	
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	خرابی‌های نرم‌افزاری	☑		
		خرابی‌های سخت‌افزاری	☑		
2	**محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.**			☑	

3	**در صورتی که محصول از محصولات امن IT دیگری استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.**			☐	با محصول دیگری در ارتباط نیست.
	داده امنیتی قلبل اشتراک‌گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.	داده‌های احراز هویت	☐		
		کلید	☐		
		امضای دیجیتال	☐		
		ثبت‌نشان‌ها (داده‌های ممیزی)	☐		
		سایر موارد	☐		
4	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[3] معتبر را تولید یا از آن‌ها استفاده نماید.**			☑	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐		
		تنظیم مهرهای زمانی از طریق اینترنت	☐		
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	☑		
		سایر موارد	☐		

[3] Time stamp

5	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**			☑	
	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروزرسانی دستی	☑		
		جستجوی خودکار بروزرسانی‌ها	☐		
		بروزرسانی‌های خودکار	☐		
		بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	☐		
6	**در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**			☐	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضای دیجیتال	☐		
		درهم‌ساز منتشرشده	☐		

7.5 تخصیص منابع

در این رده، به بررسی وضعیت عملکردهای محصول و منابع مورد استفاده توسط آن در زمانهای مختلف از جمله زمان شکست پرداخته می‌شود.

شماره الزام	رده تخصیص منابع		توضیحات
1	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	☑	

8.5 دسترسی به محصول

در این رده توانایی محصول در مدیریت نشست‌های صورت گرفته شده توسط کاربر، ارزیابی می‌شود.

شماره الزام	رده دسترسی به محصول				توضیحات
1	**محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.**			☑	
2	**محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.**			☑	
3	**محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.**			☑	
4	**در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.**			☑	
	انتخاب یک مورد لازم و کافی است.	روز	☑		
		زمان	☑		
		سایر موارد	☑		IP
5	**در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.**			☑	
		روز	☑		

	انتخاب یک مورد لازم و کافی است.	زمان	☑		
		سایر موارد	☑		IP
6	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**			☑	
7	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**			☑	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	مکان	☑		
		شماره پورت	☐		
		روز	☑		
		زمان	☐		
		سایر موارد	☐		

9.5 کانال ها/مسیرهای مورد اعتماد

در این رده به بررسی پروتکل‌های امنی که برای برقراری کانال/مسیر مورد اعتماد، بین محصول و موجودیت‌های IT خارجی، یا بین اجزای محصول، استفاده می‌شوند، پرداخته می‌شود.

شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد			توضیحات
1	**محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام دهد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد.** در صورت انتخاب مورد HTTPS، رعایت الزام **0** و **12.5** و در صورت انتخاب TLS، رعایت الزامات **11.5** تا **13.5** که در بخش **0** بیان گردیده است، الزامی است.		☑	
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	☑	
		TLS	☑	
		SSH	☐	
2	**محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.**		☑	

3	**محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.**	☑	

الزامات امنیتی مبتنی بر انتخاب

این بخش به بیان الزاماتی می‌پردازد که رعایت آنها وابسته به برخی از الزاماتی است که در بخش‌های پیشین بیان شده است. برای مثال اگر در الزامات مربوط به رده کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

10.5 پروتکل HTTPS

شماره الزام	پروتکل HTTPS		توضیحات
1	**محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.**	☑	
2	**محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.**	☑	

3	**در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید.** اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش 14.5 انجام می‌شود که در این صورت الزامات بخش 14.5 الزامی است.			☑	
	محصـــول تنها از موارد بیان‌شـــده می‌تواند اسـتفاده نماید.	اتصال را برقرار نکند.	☑		
		برای برقراری اتصال درخواست مجوز کند.	☐		

11.5 پروتکل TLS Client

شماره الزام	پروتکل TLS Client					توضیحات
1	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**				☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی‌شده محصول، انتخاب گردد.	☑	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446			
		☑	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446			
		☑	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288			
		☑	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288			
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289			
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030			

		مطابق با RFC 5289			
		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289	☑		
		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289	☑		
		TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288	☐		
		TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288	☐		
		TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288	☐		
		TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289	☐		
		TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289	☐		
		TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289	☐		
		TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288	☐		

		☐	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288		
2	**محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید نماید.**	☑			
3	**محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.**	☑			
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	☑	ارتباط را برقرار نکند		
		☐	برای برقراری ارتباط درخواست مجوز کند		
		☐	سایر موارد		
4	**محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.**	☑			
	در صورتی که محصول از خم‌های بیضوی استفاده می‌نماید، نوع	☐	Supported Elliptic Curves Extension را ارائه نکند.		
		☑	Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.		secp256r1, secp384r1, secp521r1

	خـــم بـــایـــد مشخص گردد.				

12.5 پروتکل TLS Server

شماره الزام	پروتکل TLS Server				توضیحات
1	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☐	
	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446	☐		
		TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446	☐		
		TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288	☐		
		TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288	☐		
		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289	☑		
		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289	☑		
		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	☐		

		0xC02C مطابق با RFC 5289			
		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289	☐		
		TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288	☑		
		TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288	☑		
		TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288	☐		
		TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289	☐		
		TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289	☐		
		TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289	☐		
		TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288	☐		
		TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0	☐		

		مطابق با RFC 5288			
2	**محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1دارند را رد نماید.**			☑	
3	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			☑	
	طولی کلید یا نوع خم مورد استفاده باید مشخص گردد.	استفاده از RSA با اندازه کلید 2048 یا 3072 یا 4096 بیت	☑		2048 بیت
		پارامترهای ECDH(E) با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر	☑		secp256r1, secp384r1, secp521r1
		پارامترهای دیفی-هلمن با اندازه کلید 2048 یا 3072 بیت	☐		

13.5 پروتکل TLS مشترک کلاینت و سرور

لازم به ذکر است که الزاماتی که با عنوان پروتکل‌های TLS Server و TLS Client مطرح شده است، برای مباحث مرتبط به احراز هویت TLS Server و TLS Client نیز مطرح می‌گردد. در این بخش چند الزام که برای احراز هویت این پروتکل‌ها مطرح می‌گردد و برای هر دوی کلاینت و سرور نیز یکسان است و باید برای هر کدام مورد بررسی قرار گیرد، آورده شده است.

شماره الزام	پروتکل TLS مشترک کلاینت و سرور		توضیحات
1	**محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.**	☑	
2	**در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، محصول نباید کانال امن را برقرار سازد.**	☐	محصول کلاینت ها را احراز هویت نمی کند.

14.5 اعتبارسنجی گواهی‌نامه

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
1	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			☑	
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		
		محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	☑		
	روش‌های تأیید وضعیت فسخ گواهی‌نامه	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص‌شده در RFC 696	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش 6.3	☐		

		☐	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش 5		
		☑	هیچ روش فسخ دیگری		
	قولنین تـأییـد بخش extendedKeyUsage	☐	گواهی‌نامه‌های مورد استفاده برای تأیید بروزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در بخش extendedKeyUsage خود داشته باشند.		

2	**محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.**			☑	
3	**محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند.**			☑	
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.	HTTPS	☑		
		TLS	☑		
		SSH	☐		
		امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	☐		
		امضای کد برای تأیید یکپارچگی	☐		
		سایر موارد	☐		

15.5 پروتکل SSH

شماره الزام	پروتکل SSH		توضیحات
1	**محصول باید پروتکل SSH را مطابق با RFCهای 4251، 4252، 4253، 4254، 5656 و 6668 پیاده‌سازی نماید.**	☐	
2	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.**	☐	
	☐ احراز هویت مبتنی بر کلید عمومی		
	☐ احراز هویت مبتنی بر گذرواژه		
3	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.**	☐	
4	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.**	☐	
	☐ AES128-CBC		
	☐ AES192-CBC		
	☐ AES256-CBC		
	☐ AES128-CTR		
	☐ AES192-CTR		
	☐ AES256-CTR		

		☐	AEAD_AES_128_GCM		
		☐	AEAD_AES_256_GCM		
5	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.**	☐			
		☐	ssh-ed25519		
		☐	ssh-ed448		
		☐	rsa-sha2-512		
		☐	rsa-sha2-256		
		☐	ecdsa-sha2-nistp521		
		☐	ecdsa-sha2-nistp384		
		☐	ecdsa-sha2-nistp256		
		☐	x509v3-ecdsa-sha2-nistp521		
		☐	x509v3-ecdsa-sha2-nistp384		
		☐	x509v3-ecdsa-sha2-nistp256		
		☐	x509v3-rsa2048-sha256		
		☐	ssh-rsa		
		☐	x509v3-ssh-rsa		
6	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.**	☐			
		☐	AEAD_AES_256_GCM		
		☐	AEAD_AES_128_GCM		
		☐	hmac-sha2-512		
		☐	hmac-sha2-256		
		☐	hmac-sha1-96		
		☐	hmac-sha1		

7	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.** ☐ curve25519-sha256 ☐ curve448-sha512 ☐ diffie-hellman-group-exchange-sha256 ☐ diffie-hellman-group18-sha512 ☐ diffie-hellman-group17-sha512 ☐ diffie-hellman-group16-sha512 ☐ diffie-hellman-group15-sha512 ☐ ecdh-sha2-nistp521 ☐ ecdh-sha2-nistp384 ☐ ecdh-sha2-nistp256 ☐ rsa2048-sha256 ☐ diffie-hellman-group-exchange-sha1 ☐ diffie-hellman-group14-sha256	☐	
8	**محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (طول نشست بیشتر از یک ساعت و حجم داده مبادله شده بیشتر از 1 گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.**	☐	
9	**محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با**	☐	

	کلید عمومی متناظر آن (تشریح‌شده در RFC 4251 بخش 1.7) همراه می‌کند، استفاده می‌نماید.		

6 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 میباشند 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 میکند؛ 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	برچسبگذاری 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

7 خلاصه مشخصات محصول

- به ازای تمام رویدادهای ورود و خروج موفق یا ناموفق کاربر ، تغییر کنترل های دسترسی، دانلود و آپلود فایل، دسترسی به مولفه های حساس، تغییر تنظیمات امنیتی رکوردهای ممیزی با با حداقل اطلاعات تاریخ، ساعت, IP، کاربر عامل، کاربر هدف، نوع رویداد، نوع زیر رویداد، حساسیت رویداد، سطح اهمیت رویداد، پرچم امنیتی رویداد و توضیحات مربوط به رویداد تولید می گردد. امکان جستجوی پیشرفته بر اساس تک تک اقلام یاد شده برای مدیر سامانه وجود دارد و مدیر سامانه می تواند بر اساس اقلام فوق رکوردهای ممیزی را فیلتر نموده و مرتب سازی نماید.
- امکان حذف رکوردهای ممیزی برای کاربران سامانه وجود ندارد و صرفا از طریق دسترسی مستقیم به پایگاه داده امکان تغییر یا حذف رکوردهای ممیزی میسر می باشد.
- امکان تنظیم حداکثر حجم مجاز برای رکوردهای ممیزی وجود دارد و در صورتیکه حجم داده های ممیزی از میزان تعریف شده فراتر رود، سامانه بصورت خودکار ایمیل و پیامک (در صورتیکه این سرویس ها در سامانه فعال شده باشند) و همچنین پیام داخلی برای مدیر سامانه ارسال خواهد کرد. تا زمانی که فضای خالی در پایگاه داده وجود داشته باشد، رکوردهای ممیزی در سامانه ثبت خواهند شد.
- امکان ورود به سامانه از طریق نام کاربری/کلمه عبور و همچنین با استفاده از رمز عبور یکبار مصرف وجود دارد.

شرکت بهینه سازان نرم افزار بهسان ایساتیس

- مدیر سامانه می تواند میزان پیچیدگی کلمه عبور کاربران را مشخص نماید. برای مثال حداقل و حداکثر طول کلمه عبور، الزام وجود حداقل یک حرف کوچک یا بزرگ، عدد، کاراکتر خاص هنگام تعیین کلمه عبور توسط کاربر وجود دارد.
- هر کاربر پس از ورود به سامانه می تواند سوابق ورود/خروج خود به/از سامانه را مشاهده نماید.
- در صورتیکه کاربر چند بار نام کاربری/کلمه عبور را اشتباه وارد نماید مکانیزم کپچا فعال می شود و در صورتیکه بازهم نام کاربری/کلمه عبور وارد شده وارد شود، هر بار بصورت افزایشی 20 ثانیه بیشتر از دفعه قبلی اکانت کاربر قفل می گردد.
- امکان تنظیم انواع فایل مجاز و همچنین انواع تصویر مجاز و همچنین حداکثر حجم مجاز فایل ها و تصاویر در سامانه وجود دارد.
- در صورت فراموشی کلمه عبور، با درخواست کاربر برای فراموشی کلمه عبور یک ایمیل حاوی لینک با زمان اعتبار محدود برای کاربر ارسال می شود و کاربر می تواند با استفاده از این لینک کلمه عبور جدید را تعیین نماید.
- کلمه های عبور در پایگاه داده بصورت hash ذخیره می شوند و قابل بازیابی نیستند و همچنین در صورتیکه از طریق پایگاه داده تغییر داده شوند، تغییرات توسط سامانه تشخیص داده شده و از ورود کاربر جلوگیری به عمل خواهد آمد.