به نام خدا

سند هدف امنیتی
اتوماسیون خبر صبارسانه
۸.۰

راهبران فناوری نستوه

بهمن ۱۴۰۲
۱.۰

فهرست

1 معرفی

اتوماسیون خبر صبارسانه یک نرم‌افزار جامع خبری و خبرگزاری آنلاین است که برای پاسخگویی به تمامی نیازمندی‌های یک خبرگزاری متوسط و بزرگ طراحی و پیاده‌سازی شده است. در طراحی آن قابلیت گسترش‌یافتگی افقی و عمودی مورد نظر قرار گرفته است تا هرگونه توسعه آتی با کمترین هزینه و زمان، ممکن باشد.

1.1 مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی اتوماسیون خبر صبارسانه
نسخه	۱.۰
تاریخ	۱۴۰۲/۱۱/۲۸
نویسندگان	گروه توسعه شرکت راهبران فناوری نستوه

نام شرکت	راهبران فناوری نستوه
نام محصول	اتوماسیون خبر صبارسانه
نوع محصول	برنامه کاربردی تحت وب
نسخه‌ی محصول	۸.۰

حداقل نیازمندی نرم‌افزاری/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	Linux, CentOS 7 & 8 & Stream
مدل و نسخه وب سرور	Apache 2.4 & Nginx 1.18+
مدل و نسخه پایگاه داده	MariaDB 10.3+
زبان برنامه نویسی	Java / Javascript / HTML / CSS

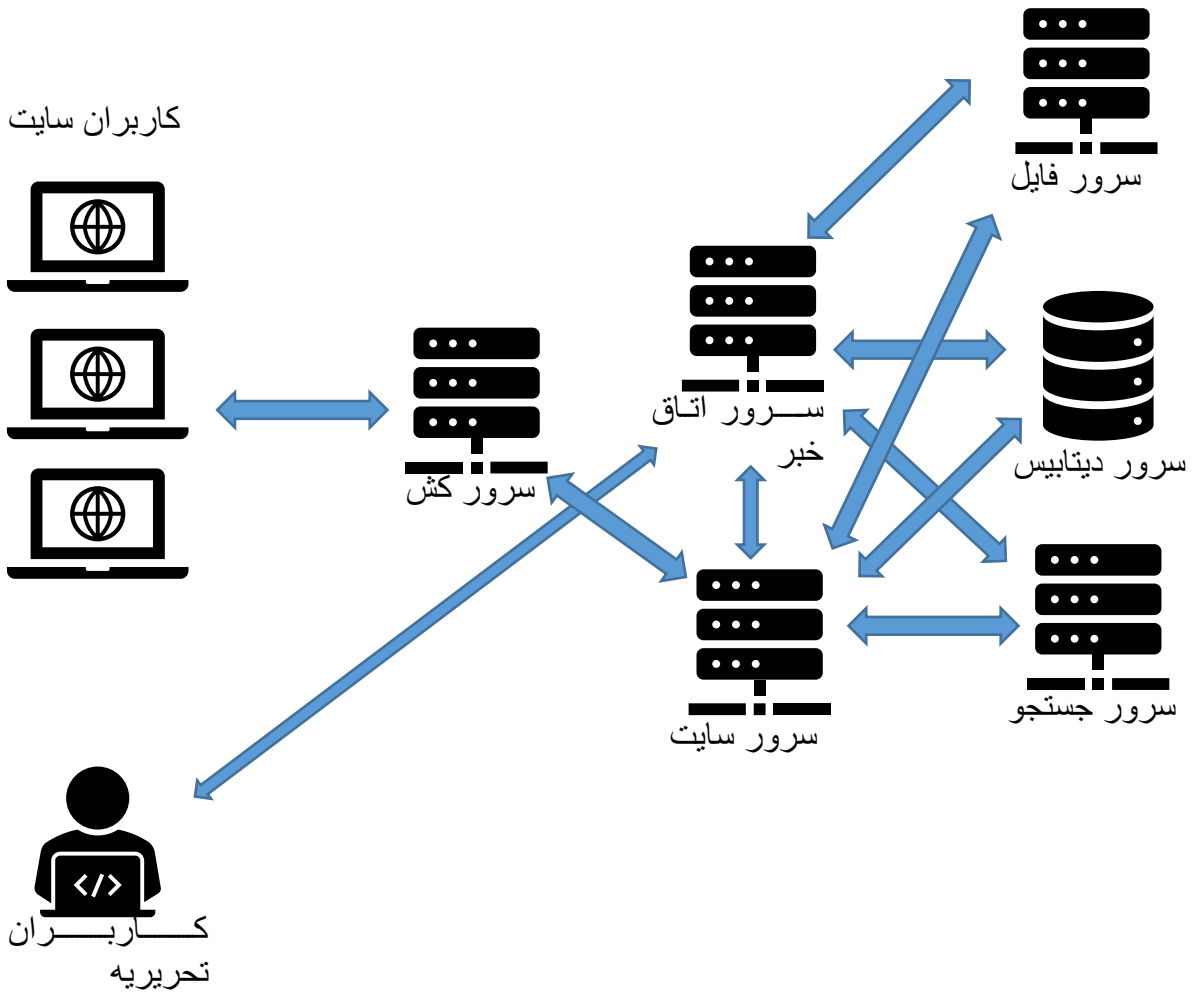
2 ادعای انطباق

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 سامانه اداری کلاینت سرور نسخه ۱.۰
سطح تضمین امنیتی	EAL1

2.2 شرح محصول

1.2.2 حوزه فیزیکی



2.2.2 حوزه منطقی

کارکردها	توصیف
احراز هویت دوعاملی	*کاربر پس از وارد کردن رمز ورود استاتیک، نهایتاً از طریق یکی از روش های پیامک، ایمیل یا TOTP، احراز هویت می‌شود.*
رویدادنگاری	*مشاهده تمامی فعالیت های انجام شده توسط کاربران*
کنترل دسترسی	*هدف ارزیابی دارای امکان دسترسی محدود میباشد، به طوریکه تنها موجودیت های مجاز خاص دارای دسترسی به داده و کارکردهای هدف ارزیابی هستند. برای کاربران مجاز کنترل دسترسی معمولا با استفاده از داده احراز هویت انجام میگیرد.*

3 مسائل امنیتی

1.3 تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم میتواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی میتواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم میتواند با سود بردن از نقض های امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم میتواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده ها میتوانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به داده ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردها، مستندات و داده های حفاظت شده توسط محصول میتواند بدون مجوز تغییر یابند. مهاجم میتواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر

تهدیدات	توضیحات
	عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم میتواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها و مستندات تضمین شده نمیباشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. و بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول میتواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول میباشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم میتواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم میتواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشای اطلاعات	داده های محرمانه که توسط محصول محافظت میشوند میتواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی میتواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی میتواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده میتواند عمداً یا غیر عمد موجب افشاء اطالعات محرمانه گردد.
انکار سرویس	مهاجم میتواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد .این امر معمولاً با ارسال درخواست های بسیار در یک بازه زمانی کوتاه صورت میگیرد طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده ای از حمله شامل ارسال درخواست های بسیار از یک رنج IP مشخص میباشد که به نام حمله DoS شناخته میشود. نوع دیگر پیشرفته تر حمله DDoS میباشد که از BOTNETاستفاده مینماید و محدودیتی بر روی آدرس IP ورودی ندارد.

تهدیدات	توضیحات
داده های ورودی مخرب	مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم میتواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر رابه دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم میتواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.

2.3 خطمشی امنیتی

خطمشی ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار میگیرند.
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLSاستفاده نمایند.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مولفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه 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 پیشفرض، خطاهای پیشفرض و صفحات 404، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار مینمایند. این خطمشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار میگیرد. بنابراین با تضمین

خطمشی ها	توضیحات
	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.

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 مینمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال مینمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ مینمایند.
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 اقدامات مناسبی صورت میگیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مولفه های سخت افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ دادهای از دست نمیرود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمیدهد.

فرضیات	توضیحات
ارتباطات	فرض شده است که تمام ارتباطات و کانال های ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال حمالتی چون DoS و شنود شبکه و غیره حفاظت میشوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حمالت DDoS اتخاذ میشود.

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 رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه نماید.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم مینماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در

هدف امنیتی	توضیحات
	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 قوی تری مدیر سیستم را احرازهویت نماید. از جمله سازوکارها میتوان به محدود نمودن رنجIP، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده های غیرمجاز را کنترل و مدیریت نماید. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست ها از یک رنج IP تعریف شده میتواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد سیستم فراهم نماید. 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 نقشها و مجوزهایی تنظیم نماید.
مدیریت خطا	محصول باید صورت امن و کارامد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات

هدف امنیتی	توضیحات
	جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده های باقیمانده	محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس میگردد.

2.4 اهداف امنیتی برای محیط عملیاتی

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 مولفه ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی میتوان به غیرفعال نمودن 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 مینمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.

هدف امنیتی	توضیحات
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله ای لازم برای تمام آسیب پذیری های امنیتی شناخته شده را در نظر میگیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه های غیر از محصول نیز مورد ممیزی قرار میگیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول میباشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور تست باید پاک یا غیر قابل 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 نماید. برای این منظور ممکن است از روال های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه 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
1	**تولید داده ممیزی ۱**	FAU_GEN.1.1
2	**تولید داده ممیزی ۲**	FAU_GEN.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
3	مرتبط نمودن هویت کاربر به رویداد ۱	FAU_GEN.2.1
4	بازبینی داده ممیزی ۱	FAU_SAR.1.1
5	بازبینی داده ممیزی محدود ۱	FAU_SAR.2.1
6	بازبینی داده ممیزی ۲	FAU_SAR.1.2
7	بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.3.1
8	انتخاب داده ممیزی ۱	FAU_SEL.1.1
9	ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
10	ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
11	اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1
12	پیشگیری از اتلاف و از دست رفتن داده ممیزی ۱	FAU_STG.4.1
13	عملیات رمزنگاری ۱ (۱)	FAU_COP.1.1(1)
14	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1(3)
15	عملیات رمزنگاری ۱ (۲)	FAU_COP.1.1(2)
16	تخریب کلید رمزنگاری ۱	FCS_CKM.4.1
17	تولید کلید رمزنگاری ۱	FCS_CKM.1.1
18	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
19	مدیریت احرازهویت ناموفق ۱	FIA_AFL.1.1
20	مدیریت احرازهویت ناموفق ۲	FIA_AFL.1.2
21	تعریف مشخصات کاربر ۱	FIA_ATD.1.1
22	مدیریت کلمه عبور	FIA_PMG_EXT.1.1
23	احراز هویت کاربر ۱	FIA_UAU.1.1
24	احراز هویت کاربر ۲	FIA_UAU.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
25	شناسایی کاربر ۱	FIA_UID.1.1
26	شناسایی کاربر ۲	FIA_UID.1.2
27	سازوکار احراز هویت چندگانه ۱	FIA_UAU.5.1
28	سازوکار احراز هویت چندگانه ۲	FIA_UAU.5.2
29	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
30	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
31	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
32	خط‌مشی کنترل دسترسی ۱	FDP_ACC.1.1
33	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
34	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
35	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
36	عملیات کنترل دسترسی ۴	FDP_ACF.1.4
37	حفاظت کامل از اطلاعات باقی‌مانده در منابع ۱	FDP_RIP.2.1
38	ورود داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.2.1
39	ورود داده کاربری به محصول با مشخصه امنیتی ۲	FDP_ITC.2.2
40	ورود داده کاربری به محصول با مشخصه امنیتی ۴	FDP_ITC.2.4
41	ورود داده کاربری به محصول با مشخصه امنیتی ۵	FDP_ITC.2.5

شماره الزام	نام الزام	تطابق الزام با استاندارد
42	ورود داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.2.3
43	خروج داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ETC.2.1
44	خروج داده کاربری به محصول با مشخصه امنیتی ۲	FDP_ETC.2.2
45	خروج داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ETC.2.3
46	خروج داده کاربری به محصول با مشخصه امنیتی ۴	FDP_ETC.2.4
47	صحت داده کاربری ذخیره‌شده ۲	FDP_SDI.2.1
48	صحت داده کاربری ذخیره‌شده ۳	FDP_SDI.2.2
49	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
50	مقداردهی اولیه مشخصه‌ها ۱	FMT_MSA.3.1
51	مدیریت مشخصه‌های امنیتی ۱	FMT_MSA.1.1
52	مقداردهی اولیه مشخصه‌ها ۲	FMT_MSA.3.2
53	مدیریت داده محصول ۱ - مدیر سیستم	FMT_MTD.1.1(1)
54	مدیریت داده محصول ۱ - کاربر عادی، واردکننده داده	FMT_MTD.1.1(2)
55	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
56	نقش‌های امنیتی ۱	FMT_SMR.1.1
57	نقش‌های امنیتی ۲	FMT_SMR.1.2
58	حفظ و امنیت وضعیت امن در زمان شکست ۱	FPT_FLS.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
59	**انتقال داده امنیتی در داخل محصول ۱**	FPT_ITT.1.1
60	**مهرهای زمانی ۱**	FPT_STM.1.1
61	**بروزرسانی امن ۲**	FPT_TUD_EXT.1.2
62	**تحمل خطا ۱**	FRU_FLT.1.1
63	**محدودیت بر روی چندین نشست هم‌زمان ۱**	FTA_MCS.1.1
64	**محدودیت بر روی چندین نشست هم‌زمان ۲**	FTA_MCS.1.2
65	**خاتمه دادن به نشست‌ها توسط محصول ۱**	FTA_SSL.3.1
66	**خاتمه دادن به نشست‌ها توسط کاربر ۱**	FTA_SSL.4.1
67	**سوابق دسترسی به محصول ۱**	FTA_TAH.1.1
68	**سوابق دسترسی به محصول ۲**	FTA_TAH.1.2
69	**سوابق دسترسی به محصول ۳**	FTA_TAH.1.3
70	**برقراری نشست ۱**	FTA_TSE.1.1
71	**مسیر امن ۱**	FTP_TRP.1.1
72	**مسیر امن ۲**	FTP_TRP.1.2
73	**مسیر امن ۳**	FTP_TRP.1.3
الزامات مربوط به پیوست اول		
74	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.1.1
75	**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.1.2
76	**الزامات پروتکل HTTPS (۳)**	FCS_HTTPS_EXT.1.3
77	**الزامات پروتکل TLS Client (۱)**	FCS_TLSC_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
78	**الزامات پروتکل TLS Client (۲)**	FCS_TLSC_EXT.1.2
79	**الزامات پروتکل TLS Client (۳)**	FCS_TLSC_EXT.1.3
80	**الزامات پروتکل TLS Client (۴)**	FCS_TLSC_EXT.1.4
81	**الزامات پروتکل TLS Server (۱)**	FCS_TLSS_EXT.1.1
82	**الزامات پروتکل TLS Server (۲)**	FCS_TLSS_EXT.1.2
83	**الزامات پروتکل TLS Server (۳)**	FCS_TLSS_EXT.1.3
84	**الزامات پروتکل TLS Server / احراز هویت (۴)**	FCS_TLSS_EXT.2.4
85	**الزامات پروتکل X509 (۱) / ابطال**	FIA_X509_EXT.1.1/Rev
86	**الزامات پروتکل X509 (۲) / ابطال**	FIA_X509_EXT.1.2/Rev
87	**الزامات پروتکل X509 (۳)**	FIA_X509_EXT.2.1
88	**الزامات پروتکل SSH (۱)**	FCS_SSH_EXT.1.1
89	**الزامات پروتکل SSH (۲)**	FCS_SSH_EXT.1.2
90	**الزامات پروتکل SSH (۳)**	FCS_SSH_EXT.1.3
91	**الزامات پروتکل SSH (۴)**	FCS_SSH_EXT.1.4
92	**الزامات پروتکل SSH (۵)**	FCS_SSH_EXT.1.5
93	**الزامات پروتکل SSH (۶)**	FCS_SSH_EXT.1.6
94	**الزامات پروتکل SSH (۷)**	FCS_SSH_EXT.1.7
95	**الزامات پروتکل SSH (۸)**	FCS_SSH_EXT.1.8
96	**الزامات پروتکل SSH (۹)**	FCS_SSH_EXT.1.9

1.5 کلاس ممیزی امنیت

شماره الزام	نام الزام
1	**تولید داده ممیزی ۱**
محصول می‌تواند برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان تولید کند (Log ثبت نماید).	

شماره الزام	نام الزام	
	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	
	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 درخواست‌های (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	

شماره الزام	نام الزام
2	**تولید داده ممیزی ۲ و مرتبط نمودن هویت کاربر به رویداد ۱**

محصول می‌تواند برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.

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	

3	**بازبینی داده ممیزی ۱ و بازبینی داده ممیزی محدود ۱**

محصول می‌تواند ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.

4	**بازبینی داده ممیزی ۲**

ثبت‌نشان‌هایی که محصول تولید می‌نماید می‌تواند برای کاربر ساده و قابل فهم باشند.

نبود داده نامفهوم در رکوردها	
نبود بخش‌های نامرتبط	
وجود داده معتبر و مناسب در هر بخش	

5	**بازبینی داده ممیزی قابل انتخاب ۱ و انتخاب داده ممیزی ۱**

محصول می‌تواند امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.

هویت موجودیت فعال	
تاریخ/زمان	
روش اتصال کاربر	
نوع رخداد	
مکان رویداد	

6	**ذخیره‌سازی رویدادهای ممیزی ۱ و ۲**

محصول می‌تواند هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.

شماره الزام	نام الزام	
	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	
	فقط خواندنی کردن ثبت‌نشان‌ها در محصول	
7	**اقدامات لازم در زمان از دست رفتن داده ممیزی ۱**	
محصول می‌تواند وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.		
	اطلاع‌رسانی از طریق نرم‌افزار مونیتورینگ (monit)	محدودیتی در حجم ذخیره‌سازی ثبت‌نشان‌ها وجود ندارد و تا زمانی که در هارد دیسک فضای کافی برای ذخیره‌سازی باشد، ثبت‌نشان‌ها ذخیره می‌شوند.
8	**پیشگیری از اتلاف و از دست رفتن داده ممیزی ۱**	
محصول می‌تواند 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.		
	پس از پر شدن فضای ثبت‌نشان‌ها (پر شدن هارد دیسک) نرم‌افزار از کار می‌افتد.	

2.5 کلاس رمزنگاری

شماره الزام	نام الزام	
9	**عملیات رمزنگاری ۱ (۱) و عملیات رمزنگاری ۱ (۳)**	
محصول می‌تواند قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام می‌دهد.		
	مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	طول کلید ۲۵۶ و ۱۲۸ بیتی
10	**عملیات رمزنگاری ۱ (۲)**	
محصول می‌تواند بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده می‌نماید.		

شماره الزام	نام الزام	
	الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت	
	الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت	
11	**تخریب کلید رمزنگاری ۱**	
تخریب کلید رمزنگاری بر اساس موارد زیر صورت می‌پذیرد.		
	از طریق توابع امنیتی محصول	
12	**تولید کلید رمزنگاری ۱ و عملیات رمزنگاری ۱ (۴)**	
سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام می‌گیرد.		
	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)	
	الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۶.۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	

3.5 کلاس شناسایی و احراز هویت

شماره الزام	نام الزام	
13	**مدیریت احرازهویت ناموفق ۱**	
محصول می‌تواند 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.		
	یک عدد مثبت ثابت	
14	**مدیریت احرازهویت ناموفق ۲**	

شماره الزام	نام الزام
محصول می‌تواند زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.	
غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	در صورت وارد کردن غلط رمز عبور برای تعداد بار مشخص به مدت معینی یوزر قفل می‌شود. رفع قفل به شکل خودکار پس از این زمان انجام می‌شود. با این حال مدیر هم میتواند به شکل فوری رفع قفل کند.
غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	در صورت وارد کردن غلط رمز عبور برای تعداد بار مشخص به مدت معینی یوزر قفل می‌شود. رفع قفل به شکل خودکار پس از این زمان انجام می‌شود. با این حال مدیر هم میتواند به شکل فوری رفع قفل کند.
استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)	در صورتی که یکبار رمز را غلط وارد کند، برای دریافت مجدد رمز کپچا لود می‌شود.
15	**تعریف مشخصات کاربر ۱**
محصول می‌تواند برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.	
شناسه کاربر	
روش احراز هویت مورد استفاده	
داده احراز هویت	
وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	
نقش کاربر	
16	**مدیریت کلمه عبور**
محصول می‌تواند قابلیت مدیریت گذرواژه را فراهم آورد.	

شماره الزام	نام الزام	
	استفاده از حروف کوچک	
	استفاده از حروف بزرگ	
	استفاده از اعداد	
	استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...)	
	حداقل طول 8 یا بیشتر (قابل تنظیم)	
17	**احراز هویت کاربر ۱ و ۲ و شناسایی کاربر ۱ و ۲**	
محصول می‌تواند پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.		
	هیچ اقدامی	
18	**سازوکار احراز هویت چندگانه ۱ و ۲**	
محصول می‌تواند از سازوکار احراز هویت پشتیبانی نماید.		
	نام کاربری و گذرواژه	
	احراز هویت دو فاکتوری	
19	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**	
محصول می‌تواند برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.		
	شناسه کاربر	
	نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	
	جزئیات واسط کلاینت	
	پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	
20	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**	
محصول می‌تواند در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.		
	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، به صفحه کاربر اصلی (نشست اول) اطلاع داده می‌شود.)	

شماره الزام	نام الزام
	بروزرسانی اطلاعات پیشینه احراز هویت
21	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**
محصول می‌تواند بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.	
	غیرمجاز بودن هرگونه تغییر در طول نشست فعال

4.5 کلاس حفاظت از داده‌ی کاربری

شماره الزام	نام الزام
22	**خط‌مشی کنترل دسترسی ۱**
محصول می‌تواند برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.	
	مدیر سیستم
	کاربر عادی
	سوابق، مستندات و فراداده
	داده متعلق به کاربران
	داده احراز هویت
	ایجاد موجودیت غیرفعال جدید
	حذف موجودیت غیرفعال
	تغییر دسترسی‌ها به موجودیت غیرفعال
	عملیات بر روی فراداده وابسته به موجودیت غیرفعال
23	**عملیات کنترل دسترسی ۱**
محصول می‌تواند بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	
	نقش‌ها و مجوزهای کاربر مجاز
	اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.
24	**عملیات کنترل دسترسی ۲ و ۳**
محصول می‌تواند بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید.	

شماره الزام	نام الزام
25	**عملیات کنترل دسترسی ۴**

محصول می‌تواند بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.

عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	
از طریق نقش‌های امنیتی	

26	**حفاظت کامل از اطلاعات باقی‌مانده در منابع ۱**

محصول می‌تواند 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.

27	**ورود داده کاربری به محصول با مشخصه امنیتی ۱ و ۲ و ۴ و ۵**

محصول می‌تواند هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.

نوع داده	پسوندهای مجاز به شکل سفارشی‌شدنی تنظیم می‌شود و جلوی ارسال بقیه فایل‌ها گرفته می‌شود. به شکل پیش‌فرض یک سری از پسوندها بلک‌لیست شده‌اند.
حجم و اندازه	سیاست محدودیت حجم بر اساس تنظیمات مدیر اعمال می‌شود.
فرمت	فرمت‌های زیر به طور پیش‌فرض غیرمجاز هستند: ins, inf, js, cmd, bat, exe, com, mst, msp, msi, msc, jse, job, inx, vbe, vb, reg, ps1, pif, paf, osx, sct, scr, wsg, wsf, ws, vb, vbs, html, script, cpl, app, command, body htm,

28	**ورود داده کاربری به محصول با مشخصه امنیتی ۳**

محصول می‌تواند از یک پروتکل امن (TLS 1.2+) 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.

شماره الزام	نام الزام
29	**خروج داده کاربری به محصول با مشخصه امنیتی ۱ و ۲ و ۳**

محصول می‌تواند هنگام انتقال داده به بیرون از محصول، خطمشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.

توضیحات بخش آپلود عینا تکرار شده‌است زیرا امکان دانلود فایل‌های آپلودشده وجود دارد.

نوع داده	پسوندهای مجاز به شکل سفارشی‌شدنی تنظیم می‌شود و جلوی ارسال بقیه فایل‌ها گرفته می‌شود. به شکل پیش‌فرض یک سری از پسوندها بلک‌لیست شده‌اند.
حجم و اندازه	سیاست محدودیت حجم بر اساس تنظیمات مدیر اعمال می‌شود.
فرمت	فرمت‌های زیر به طور پیش‌فرض غیرمجاز هستند: ins, inf, js, cmd, bat, exe, com, mst, msp, msi, msc, jse, job, inx, vbe, vb, reg, ps1, pif, paf, osx, sct, scr, wsg, wsf, ws, vb, vbs, html, script, cpl, app, command, body htm,

30	**خروج داده کاربری به محصول با مشخصه امنیتی ۴**

محصول می‌تواند هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.

مدیر سیستم می‌تواند خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	

31	**صحت داده کاربری ذخیره‌شده ۲**

محصول می‌تواند تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.

مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	

32	**صحت داده کاربری ذخیره‌شده ۳**

شماره الزام	نام الزام
محصول می‌تواند در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.	
ایجاد هشدار/اخطار برای نقش‌های مجاز	

5.5 کلاس مدیریت امنیت

شماره الزام	نام الزام
33	**مدیریت کارکرد در محصول ۱ و مقداردهی اولیه مشخصه‌ها ۱**
محصول می‌تواند 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.	
تعیین و تغییر رفتار	
غیرفعال نمودن	
فعال نمودن	
34	**مدیریت مشخصه‌های امنیتی ۱**
محصول می‌تواند 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	
تغییر	
حذف	
تغییر پیش‌فرض	
35	**مقداردهی اولیه مشخصه‌ها ۲ و مدیریت داده محصول ۱ - مدیر سیستم و مدیریت داده محصول ۱ - کاربر عادی، واردکننده داده**
محصول می‌تواند برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.	
تغییر پیش‌فرض	
حذف نمودن	
پرس‌وجو	

شماره الزام	نام الزام	
مقداردهی		
ایجاد		
مشاهده		
36	**کارکردهای مدیریتی محصول ۱**	

محصول می‌تواند توانایی انجام کارکردهای زیر را داشته باشد.

پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	
پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	
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)	این مورد توسط JVM و سیستم عامل هندل می‌شود.
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 صورت می‌گیرد.	
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	

شماره الزام	نام الزام
	مدیریت نقش‌ها در محصول
	مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر
37	**نقش‌های امنیتی ۱**
محصول می‌تواند توانایی تعریف نقش‌های مختلف را داشته باشد.	
	مدیر سیستم
	کاربر پیشرفته
	کاربر عادی
38	**نقش‌های امنیتی ۲**
محصول می‌تواند کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین هر حساب کاربری تنها به یک نقش مرتبط شده است، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.	

6.5 کلاس حفاظت از توابع امنیتی محصول

شماره الزام	نام الزام
39	**حفظ و امنیت وضعیت امن در زمان شکست ۱**
محصول می‌تواند 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.	
	خرابی‌های نرم‌افزاری
	خرابی‌های سخت‌افزاری
40	**انتقال داده امنیتی در داخل محصول ۱**
محصول می‌تواند از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	
41	**مهرهای زمانی ۱**

شماره الزام	نام الزام
محصول می‌تواند زمان و تاریخ معتبری داشته باشد، بنابراین مهرهای زمانی معتبر را تولید یا از آن‌ها استفاده می‌نماید.	
تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	
42	**بروزرسانی امن ۲**
محصول می‌تواند امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.	
بروزرسانی دستی	

7.5 کلاس تخصیص منابع

شماره الزام	نام الزام
43	**تحمل خطا ۱**
محصول می‌تواند در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	

8.5 کلاس دسترسی به محصول

شماره الزام	نام الزام
44	**محدودیت بر روی چندین نشست هم‌زمان ۱ و ۲**
محصول می‌تواند حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	
45	**خاتمه دادن به نشست‌ها توسط محصول ۱**
محصول می‌تواند کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (که توسط مدیر قابل تنظیم است،) خاتمه دهد.	
46	**خاتمه دادن به نشست‌ها توسط کاربر ۱**
محصول می‌تواند به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	
47	**سوابق دسترسی به محصول ۱**

شماره الزام	نام الزام
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول می‌تواند قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.	
روز	
زمان	
48	**سوابق دسترسی به محصول ۲**
در صورت برقراری نشست به طور موفقیت آمیز، محصول می‌تواند قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.	
روز	
زمان	
مقدار آی‌پی نیز برای آخرین تلاش ناموفق نمایش داده می‌شود.	
49	**سوابق دسترسی به محصول ۳**
محصول نمی‌تواند اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.	
50	**برقراری نشست ۱**
محصول می‌تواند توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.	
مکان	
زمان	
کشور	

9.5 کلاس کانال‌ها/مسیرهای مورد اعتماد

شماره الزام	نام الزام
51	**مسیر امن ۱**
محصول می‌تواند 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.	

شماره الزام	نام الزام	
	HTTPS	
	TLS	
	SSH	
52	مسیر امن ۲	
محصول می‌تواند به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.		
53	مسیر امن ۳	
محصول می‌تواند استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.		

6 الزامات تضمین امنیت

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

7 خلاصه مشخصات محصول

نسخه ۱.۰ سند هدف امنیتی سیستم اتوماسیون خبر صبارسانه توسط کمیته توسعه شرکت راهبران فناوری نستوه تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است.

• محصول می تواند برای تمام رویدادهای ورود و خروج کاربر به/ از سیستم، کنترل دسترسی، مشخصه های امنیتی و دیگر رویدادهای قابل ممیزی رکورد ممیزی تولید نماید و برای هر رکورد ممیزی، حداقل اطلاعات تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد، نوع کاربری، IP کاربر، محل خدمت کاربر زیر را ثبت نماید و کاربر عامل هر یک از رویدادهای سیستم را شناسایی و ثبت کند.

• محصول دارای قابلیت خواندن/مشاهده ورود موفق، ورود ناموفق، تعلیق ورود، ویرایش، حذف و ایجاد آیتم جدید، صدور مجوز و گواهینامه، تکمیل فرم و تصحیح اطلاعات از کل رکوردهای ممیزی را برای مدیر سیستم و دارای قابلیت نمایش رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر میباشد و میتواند از خواندن رکوردهای ممیزی توسط کاربران غیر مجاز جلوگیری کرده و امکان انجام مرتب سازی رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس مرکز برگزار کننده، کاربر، نوع کاربری، تاریخ، موضوع و نوع رخداد (عملیات) مرتب نماید.

• از طریق خود نرم افزار امکان حذف غیر مجاز داده ممیزی وجود ندارد. کاربر تنها در صورتی امکان حذف داده ممیزی را دارد که به صورت غیر مجاز به پایگاه داده دسترسی داشته باشد و از آنجا عملیات حذف را انجام دهد که در آن حالت عملیات پیش گفته در پایگاه داده به طور خودکار ممیزی می شود. در صورت تجاوز دنباله ممیزی از مقدار حجم تعریف شده اولیه میتواند حجم مورد نظر را به صورت خودکار و مقداری که از پیش تعیین شده افزایش دهد. در صورت درخواست سازمان طرف قرار داد می توان MailServer برای پایگاه داده تعریف کرد که اگر حجم درایو کمتر از ۱۰۰ مگابایت (یا حجم مشخص دیگری) باقیمانده بود ایمیلی مبنی بر عدم وجود حجم کافی برای ذخیره سازی داده ممیزی به مدیر سیستم ارسال شود.

• می توان بر اساس مشخصه های شعبه، گروه کاربری، محدوده زمانی، موضوع، فرم و IP مجموعه از رویدادها را جهت ممیزی نمودن انتخاب نمود.

• محصول می تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتمهای تولید کلید استاندارد "استفاده از طرح RSAبا اندازه کلید ۲۰۴۸ بیت یا بیشتر که از اسناد PUB FIPS ،4-186 DSS)" "Signature Digital Standard)، " B Appendix.3.پیروی میکند تولید کنند و رمزنگاری و رمزگشایی را مطابق با با ، F38-800NIST SPسند مطابق AES Key Wrap with Paddi ng (KWP متقارن رمزنگاری الگوریتم اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.

• می توان با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نموده و حداکثر تعداد ورود ناموفق نام کاربری و گذرواژه را در سیستم تعریف کرد.

• محصول باید مشخصه های امنیتی شناسه کاربر داده های احراز هویت، نقش کاربر، وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)، IP کاربر، رمز عبور کاربر و ایمیل کاربر را برای هر کاربر نگهداری نماید.

• می توان قبل از وارد کردن نام کاربری و گذرواژه از امکان بازیابی رمز عبور استفاده کرده و هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نمود و اقدامات دریافت نام کاربری و کلمه عبور و احراز هویت از طریق Active Directory را برای احرازهویت کاربر فراهم آورد.

• محصول می تواند مشخصه های امنیتی شناسه کاربر، نقش های کاربر، جزئیات واسط کلاینت (مرورگر، IP)، پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق) تا ۳۰ دقیقه گذشته، پیشینه دسترسی به سند/رکورد اخیر(ممیزی)، کد ملی کاربر و ایمیل کاربر را برای کاربر فعال نگهداری نماید.

o زمانیکه یک نشست جدید برقرار می شود، اطلاعات موجود از نشست های قبلی حذف میگردد. اطلاعات پیشینه احراز هویت بروزرسانی میشود. رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید ثبت میگردد.

• محصول می تواند هنگام دریافت داده کاربری حداکثر حجم تصویر، فرمت های مجازکد ملی ۱۰ رقمی صحیح را اعمال کرده و از مشخصه های امنیتی مرتبط با داده های کاربری را هنگام ورود داده ها استفاده نماید.

• محصول میتواند هنگام خروج داده کاربری به بیرون داده ها را در سه فرمت (pdf, word, excel) نمایش داده و از خروج داده های حساس مانند نام کاربری و کلمه عبور و ایمیل کاربر جلوگیری کند. امکان نگهداری داده کاربری حساس ذخیره شده در مکان تحت کنترل براساس مشخصه های رمزنگاری امن نگهداری کرده و آنها را به منظور شناسایی خطای صحت داده رکورد و داده ممیزی پایش کند.

• سیستم 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 مانند ایجاد، تغییر، ویرایش و حذف موجودیت های فعال و غیرفعال اعمال نماید.

• محصول می تواند سطح دسترسی را با توجه به هویت کاربر، نقش ها و مجوزهای کاربر مجاز و اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند، بر روی موجودیت های غیرفعال اعمال نماید.

• سیستم دارای قابلیت محدودسازی توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر می باشد.

• می توان با اعمال تعیین سطح دسترسی بر اساس نقش ، توانایی تغییر پیشفرض، پرس و جو، تغییر، حذف، ایجاد مشخصه های امنیتی نام کاربری و کلمه عبور را به مدیر سیستم محدود نمود و امکان در نظرگرفتن مقادیر پیش فرض محدود شده محصول برای مشخصه های امنیتی که برای اعمال خط مشی استفاده می شوند، وجود داشته و مدیر سیستم از طریق فایل Config می تواند هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد.

• محصول می تواند توانایی تغییر پیشفرض، 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 پیشفرض، پرس و جو، تغییر پسورد به کاربر عادی محدود نماید.

• محصول می تواند به انجام کارکردهای می باشد و می توان در هر یک از ماژول های سیستم نقش های مورد نیاز را تعریف نمود.

• سیستم می تواند کاربران را با نقشهای مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود کند.

• در صورت رخ دادن هرگونه شکستی کاربر عادی خطای کلی را می بیند و مدیر از روی سرور جزئیات و منشأ پیغام را مشاهده می نماید. بنابراین در صورت شکست سیستم همواره در وضعیت امن باقی خواهد ماند.

• اشتراک گذاری داده های امنیتی بین محصول و دیگر محصولات امن IT از طریق مکانیسم احراز هویت مرکزی با استفاده از روش هایی نظیر Active Directory و احراز هویت مرکزی CAS در سازمان مشتری انجام می گیرد.

• محصول می تواند هنگام انتقال داده ها بین بخشهای 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 تعاملی راه دور را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد و اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.

• در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست براساس روز، زمان می باشد.

• محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل HTTPS، TLS میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احرازهویت که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از دادههای تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند اجازه داشته باشد به موجودیتهای معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند و تمامی بخش های سیستم. سازگاری کامل با پروتکل های امن SSL و غیره را دارند.