به نام خدا

سند هدف امنیتی

[سیستم های منابع انسانی سیمرغ ۳۴۰۰۰]

[نرم افزار مدیریت جامع منابع انسانی-۱.۲.۳.۱]

[شهریور -۱۴۰۱]
[۱.۳.۸]

فهرست

[این بخش سند هدف امنیتی بیانگر مشخصات کلی **معرفی** محصول می‌باشد. در این قسمت باید دیدکلی از محصول ارزیابی شده ارائه گردد.]

مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف سامانه مدیریت جامع منابع انسانی سیمرغ ۳۴۰۰۰
نسخه	۱.۰
تاریخ	مرداد ۱۴۰۳
نویسندگان	گروه توسعه شرکت سیستم های منابع انسانی سیمرغ ۳۴۰۰۰

نام شرکت	توسعه شرکت سیستم های منابع انسانی سیمرغ ۳۴۰۰۰
نام محصول	سامانه مدیریت جامع منابع انسانی سیمرغ ۳۴۰۰۰
نوع محصول	برنامه کاربردی تحت وب
نسخه‌ی محصول	۱.۲.۳.۱

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
پردازنده	8 Core CPU 2.1 GHz or Higher
فضای آزاد دیسک	300GB
حافظه	16GB or Higher
سیستم عامل	Windows server 2022
DBMS	Microsoft SQL Server 2019
سایر نرم افزارها	SQL Server Management Studio v20 or Higher. Web server(IIS). Net Framework 4.8 dotnet-hosting-۸.۰.۴ Module Rewrite_amd64_en-US

ادعای انطباق

در این قسمت باید انطباق سند هدف ارزیابی با موارد مطرح شده در جداول زیر مشخص شود، برای اطلاعات بیشتر جهت تکمیل این قسمت به بخش ۱.۲ از سند «راهنمای نوشتن سند هدف امنیتی» مراجعه شود.

انطباق با استاندارد ارزیابی امنیتی معیار مشترک

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

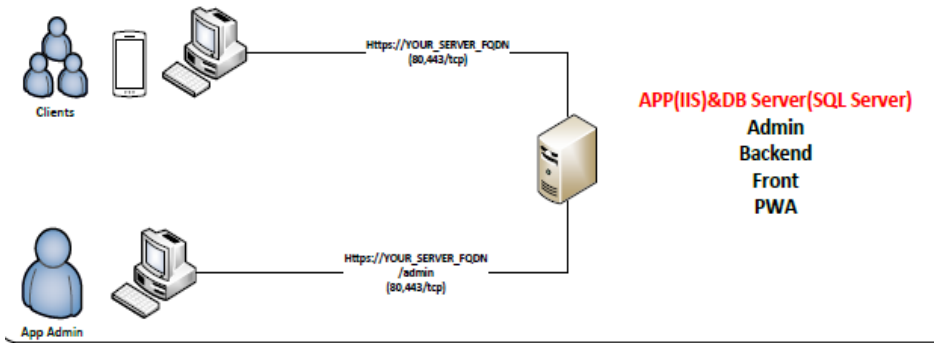
[در این قسمت محصول و کارکرد امنیتی آن به **شرح محصول** همراه کامپونت‌های اصلی در حدود ۲ تا ۳ پاراگراف شرح داده می‌شود.]

۱,۲,۲ حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه

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



۲,۲,۲ حوزه 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 استفاده از Active Deirectory	ارتباط نرم افزار با سرور Directory Active و شناسایی هویت فرد
Login به نرم افزار با استفاده از SSO	ارتباط با SSO مشتری ها و شناسایی هویت افراد
رویداد نگاری	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 دستتترستتی معموال با استتتفاده از داده احراز هویت انجام میگیرد

[این فصل تنها کافیست از سند پروفایل **مسائل امنیتی** حفاظتی کپی گردد.]

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 نقضهای امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم میتواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این دادههای میتوانند دادههای حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به دادهها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و دادههای حفاظت شده توسط محصول میتواند بدون مجوز تغییر یابند. مهاجم میتواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم میتواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر دادههای حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها

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

خط‌مشی امنیتی

خط مشی 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 TLS استفاده نمایند.
پیکربندی مناسب	پیکربندی پیشفرض محصول و مولفههای تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویسهایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیشفرض، خطاهای پیشفرض و صفحات ۴۰۴ ، مقادیر احراز هویت پیشفرض، نام کاربری پیشفرض، پورتهای پیشفرض، صفحات پیشفرض که اطلاعات داخلی همچون شماره نسخه را آشکار مینمایند. این خطمشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار میگیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی میتوان از 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.

فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیدهاند و قوانین را دنبال مینمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول)همانند برنامه نویس، طراح، غیره (افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال مینمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیبپذیریهای شناخته شده را اتخاذ مینمایند.
محیط امن	فرض شده است که تمام پیشبینیهای محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری

فرضیات	توضیحات
	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 داده ای از دست نمیرود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمیدهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانالهای ارتباطی مورد استفاده توابع امنیتی محصولجهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال حملاتی چون DoS و شنود شبکه و غیره حفاظت میشوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ میشود.

[این فصل تنها کافیست از سند پروفایل **اهداف امنیتی** حفاظتی کپی گردد.]

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.

هدف امنیتی	توضیحات
	محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم مینماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احرازهویت نماید. از جمله سازوکارها میتوان به محدود نمودن رنج IP ، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
کنترل جریان داده	محصول باید گردش دادههای غیرمجاز را کنترل و مدیریت نماید. دادههای ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنج IP تعریف شده میتواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
صحت داده	محصول باید نسبت به صحت داده ممیزی و دادهی رکورد با تشخیص هرگونه تغییر بر روی این 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 واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقشهای کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید.

هدف امنیتی	توضیحات
مدیریت خطا	محصول باید صورت امن و کارامد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صور رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده های باقیمانده	محصول باید اطمینان دهد که هر دادهی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس میگردد.

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 مولفهها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفههای 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 سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانههای ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهندهی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابلهای لازم برای تمام آسیبپذیریهای امنیتی شناخته شده را در نظر میگیرد

هدف امنیتی	توضیحات
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 دادههای باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روالهای از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفههای سختافزاری نیز نسخه پشتیبان تهیه گردد.

الزامات کارکرد امنیتی محصول مطابق با **الزامات کارکرد امنیتی** 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	بازبینی داده ممیزی ۲	FAU_SAR.1.2
٤	بازبینی داده ممیزی ۴	FAU_SAR.3.1
٥	ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.1.1
٦	ذخیره سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۷	ذخیره سازی رویدادهای ممیزی ۷	FAU_STG.4.1
۸	عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱	FCS_COP.1.1(1)
۹	عملیات رمزنگاری ۱	FCS_COP.1.1(2)
۱۰	مدیریت کلید رمزنگاری	FCS_CKM.1.1
۱۱	مدیریت کلمه عبور	FIA_PMG_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۲	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
۱۳	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
۱٤	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۱٥	**شناسایی کاربر ۱**	FIA_UID.1.1
۱٦	**احراز هویت کاربر ۱**	FIA_UAU.1.1
۱۷	**احراز هویت کاربر ۲**	FIA_UAU.1.2
۱۸	**مشخصه های امنیتی کاربر ۱**	FIA_USB.1.1
۱۹	**مشخصه های امنیتی کاربر ۲**	FIA_USB.1.2
۲۰	**خط مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۲۱	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۲۲	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۲۳	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۲٤	**ورود داده های کاربری به محصول ۴**	FDP_ITC.2.1
۲٥	**ورود داده های کاربری به محصول ۵**	FDP_ITC.2.2
۲٦	**خروج داده های کاربری از محصول ۳**	FDP_ETC.2.1
۲۷	صحت داده های کاربری ذخیره شده ۱	FDP_SDI.2.1
۲۸	صحت داده های کاربری ذخیره شده ۲	FDP_SDI.2.2
۲۹	**مدیریت کارکرد در محصول ۱**	FMT_MOF.1.1
۳۰	**مدیریت داده های محصول ۱**	FMT_MTD.1.1(2)
۳۱	**مدیریت داده های محصول ۱-مدیر سیستم**	FMT_MTD.1.1(1)
۳۲	**کارکردهای مدیریتی محصول ۱**	FMT_SMF.1.1
۳۳	نقش های امنیتی ۱	FMT_SMR.1.1
۳٤	نقش های امنیتی ۲	FMT_SMR.1.2
۳٥	**حفظ وضعیت امن در زمان شکست ۱**	FPT_FLS.1.1
۳٦	**انتقال داده امنیتی در داخل محصول ۱**	FPT_ITT.1.1
۳۷	**مهرهای زمانی ۱**	FPT_STM.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۸	**به روز رسانی امن ۲**	FPT_TUD_EXT.1.2
۳۹	**محدودیت بر روی چندین نشست همزمان ۱**	FTA_MCS.1.1
٤۰	**محدودیت بر روی چندین نشست همزمان ۲**	FTA_MCS.1.2
٤۱	**قفل کردن و خاتمه دادن به نشست ها ۵**	FTA_SSL.3.1
٤۲	**قفل کردن و خاتمه دادن به نشست ها ۶**	FTA_SSL.4.1
٤۳	**سوابق دسترسی به محصول ۱**	FTA_TAH.1.1
٤٤	**کانال امن ۱**	FTP_ITC.1.1
٤٥	**کانال امن ۲**	FTP_ITC.1.2
٤٦	**کانال امن ۳**	FTP_ITC.1.3
الزامات مربوط به پیوست اول		
۴۷		

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

محصول باید برای موارد مشخص شده که در ذیل آمده است، رکورد ممیزی تولید کند:

- **شروع و اتمام توابع**
- **تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ**
- **خواندن اطلاعات از رکوردهای لاگ**
- **تمامی تغییرات در پیکربندی لاگ**
- **عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه**
- **عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها**
- **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 کلمه عبور تست شده توسط محصول**

شماره الزام	نام الزام
• شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکت و موفقیت ایجاد موجودیت فعال) • تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی • تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول • تمامی تلاش‌ها برای وارد کردن داده‌های کاربری • (شامل هرگونه مشخصه‌های 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، نمی‌توانند عملیات موردنظر را انجام دهند. • تلاش موفق یا ناموفق برای برقراری نشست. • عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل) • خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست • خاتمه به نشست غیرفعال توسط مدیر سیستم	
۲	تولید داده ممیزی ۲
محصول می تواند برای هر رکورد ممیزی تولید شده، مشخصاتی که درذیل آمده است را ثبت نماید. • تاریخ و زمان رویداد • نوع رویداد • هویت ایجادکننده رویداد • نتیجه رویداد • آدرس IP ایجادکننده رویداد	
۳	تولید داده ممیزی ۳
محصول می تواند رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.	

شماره الزام	نام الزام
۴	تولید داده ممیزی ۴
رکوردهای ممیزی که محصول تولید مینماید برای کاربر ساده و قابل فهم هستند. مواردی که در رکوردهای ممیزی وجود دارند: • عدم وجود داده نامفهوم در رکوردها • عدم وجود فیلدهای نامرتبط • وجود داده معتبر و مناسب در هر فیلد	
۵	بازبینی داده ممیزی ۱
محصول می تواند امکان انتخاب و مرتب‌سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید. • هویت موجودیت فعال • تاریخ/زمان • نوع رخداد • مکان رویداد	
۶	ذخیره سازی رویدادهای ممیزی ۱
محصول می تواند هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی راتشخیص دهد و در صورت امکان جلوگیری نماید. • فقط خواندنی کردن ممیزیها در محصول	
۷	ذخیره سازی رویدادهای ممیزی ۲
محصول می تواند وقتی که حجم داده‌های ممیزی، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید. • ارسال پیام	
۸	ذخیره سازی رویدادهای ممیزی ۳
محصول می تواند توانایی ممیزی ثبت لاگ هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و مدیر سامانه امکان تعیین سیاست برای زمان پر شدن حافظه لاگ را دارد و می	

شماره الزام	نام الزام
تواند تعیین نمایند که آیا استفاده از سامانه متوقف شده و یا با نادیده گرفتن لاگ به فعالیت خود ادامه دهد.	

کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	**عملیات رمزنگاری ۱**
محصول می تواند قابلیت رمزنگاری یا ماژول 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)	
۲	**عملیات رمزنگاری ۲**
محصول می تواند بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (هش) را دارد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده می نماید. الگوریتم SHA-256 : با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ الگوریتم SHA-384 : با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲	
۳	**تولید کلید رمزنگاری ۱**
با توجه به اینکه تولید کلید رمزنگاری در محصول وجود دارد، تخریب کلید رمزنگاری نیز از طریق توابع امنیتی محصول صورت می پذیرد.	
۴	**عملیات رمزنگاری ۳**
با توجه به اینکه امضاء دیجیتال در محصول پشتیبانی می‌شود، سرویس‌های امضاء رمزنگاری تولید و تائید) بر اساس الگوریتم‌های رمزنگاری زیر انجام می گیرد. الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر بر اساس FIPS PUB 186-4، استاندارد امضاء 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	

کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۱	**مدیریت احراز هویت ناموفق ۱**
محصول باید بتواند تعداد تلاشهای ناموفقی را که برا ی احراز هویت شدن صورت گرفته است)در هر بخش یا قسمتی که نی از به احراز هویت وجود دارد(، بر اساس موارد زیر مشخص نماید. یک عدد مثبت قابل تنظیم توسط مدیر	
۲	**مدیریت احراز هویت ناموفق ۲**
محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید. غیرفعال کردن حساب کاربری فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد. استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... در قسمت توضیحات بیان شود.	

۳	**تعریف مشخصات کاربر**
محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید. شناسه کاربر روش احراز هویت مورد استفاده داده احراز هویت وضعیت حساب کاربری)فعال، غیرفعال، بیوکه شده و غیره(نقش کاربر	
۴	**مدیریت کلمه عبور**
محصول باید قابلیت مدیریت کلمه عبور را فراهم آورد. استفاده از حروف کوچک استفاده از حروف بزرگ استفاده از اعداد استفاده از کاراکترهای خاص "@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "" , ")" و ...) حداقل طول ۸ یا بیشتر قابل تنظیم)	

۵	**مدیریت احراز هویت کاربر ۱**
محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید. هیچ اقدامی	
۶	**مدیریت احراز هویت کاربر ۲**
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). نام کاربری و کلمه عبور Active Directory	
۷	**مشخصه های امنیتی کاربر ۱**
محصول باید برای هر کاربر فعال، مشخصه‌های امنیتی 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) سایر موارد	
۸	**مشخصه های امنیتی کاربر ۲**
محصول باید 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 جزء مواردی که فعال بودن همزمان چندین نشست موردنیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی نشست اول) اطلاع داده شود.) به‌روزرسانی اطلاعات پیشینه احراز هویت	
۹	**تعریف مشخصات کاربر ۱**
محصول بر روی تغییرات مشخصه‌های امنیتی کاربر فعال قوانینی را اعمال می نماید و در صورت ویرایش کاربر، نشست فعال منقضی می‌شود.	

کلاس حفاظت از داده ی کاربری

۱	**خط مشی کنترل دسترسی**

محصول می تواند برای موجودیتها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید. موجودیت فعال : مدیر سیستم کاربر عادی موجودیت غیرفعال : رکوردها، مستندات و فراداده داده متعلق به کاربران داده احراز هویت عملیات : ایجاد موجودیت غیرفعال جدید حذف موجودیت غیرفعال تغییر دسترسیها به موجودیت غیرفعال عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال	
۲	**خط مشی کنترل دسترسی ۲**
محصول می تواند بر اساس نقش‌ها و مجوزهای کاربر مجاز، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	
۳	**عملیات کنترل دسترسی ۱**
محصول می تواند بر اساس قاعده‌های عملیات بین موجودیت فعال تحت‌کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید، این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد).	
۴	**عملیات کنترل دسترسی ۲**
محصول بر اساس قوانین زیر، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید. تجاوز چندین نشست آغاز شده با نام کاربری مشابه ازمقدار آستانه از پیش تعریف شده	
۵	**عملیات کنترل دسترسی ۳**
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.	

۶	**خط مشی کنترل دسترسی ۳**
محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند. نوع داده حجم و اندازه فرمت	
۷	**ورود داده های کاربری به محصول**
محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید.https **این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گمشدن داده حین انتقال جلوگیری می‌کند.**	
۸	**خروج داده های کاربری از محصول ۱**
محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند. پسوندهای مجاز برای خروجی های نرم افزار فقط docx, pdf , xls می باشد.	
۹	**خروج داده های کاربری از محصول ۲**
محصول باید هنگام خروج داده کاربری به خارج از محصول ، قوانینی را اعمال نماید. مدیر سیستم باید خروج رکوردها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند. فقط مدیر سامانه یا افراد مجاز امکان خروج اطلاعات از سامانه را دارند.	
۱۰	**صحت داده های کاربری ذخیره شده ۱**
محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره شده در محصول تشخیص دهد. درهم شده داده‌های کاربری ذخیره شده، نگهداری می‌شود	
۱۱	**صحت داده های کاربری ذخیره شده ۲**
محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد. ایجاد هشدار/اخطار برای نقش‌های مجاز	

مدیریت امنیت

۱	**مدیریت کارکرد در محصول**

محصول می تواند 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. **غیرفعال نمودن** **فعال نمودن**	
۲	**مدیریت داده های محصول**
محصول می تواند با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس .Error! Reference source not found**، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.** **پرس‌وجو** **تغییر** **حذف** **تغییر پیش‌فرض**	
۳	**مدیریت داده های محصول ۱-مدیر سیستم**
محصول می تواند 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 مقداردهی ایجاد مشاهده	
۴	**کارکردهای مدیریتی محصول ۱**
محصول توانایی انجام کارکردهای زیر را دارد: پشتیبانی از حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی پشتیبانی از حد آستانه و عملیات حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی 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) ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول در نظر گرفتن یک عملیات از پیش تعیین شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد. مدیریت حد آستانه برای تلاشهای ناموفق مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. مدیریت معیارها برای تنظیم کلمات عبور مدیریت داده های احراز هویت توسط مدیریا کاربر مربوطه مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام میشوند. مدیریت سازوکارهای احراز هویت مدیریت قوانین مرتبط با احراز هویت مدیریت تغییرات و فرایندهایی مانند اختصاص آدرسIP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد. مدیر مجاز می‌تواند مشخصه‌های 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 همزمانکاربران توسط مدیر مدیریت شرایط آغاز نشست توسط مدیر مجاز تعیین زمان غیرفعال بودن برای یک کاربرمشخص که پس از آن، نشست آن کاربر خاتمه یابد. تعیین زمان پیشفرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	
۵	**نقش های امنیتی**
محصول توانایی تعریف نقش های مختلف را دارد: مدیر سیستم کاربر پیشرفته کاربر عادی سایر موارد	
۶	**نقش های امنیتی**

محصول قادر است کاربران را به نقش‌های تعریف شده 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.

حفاظت از توابع امنیتی محصول

۱	**حفظ وضعیت امن در زمان شکست**
محصول می تواند هنگام رخ دادن هرگونه شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید. **شکست‌های نرم‌افزاری** **شکست‌های سخت‌افزاری**	
۲	**انتقال داده امنیتی در داخل محصول**
محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی محافظت از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	
۳	**مهرهای زمانی**
محصول زمان و تاریخ معتبری دارد، بنابراین مهره‌های زمانی معتبر، تولید یا استفاده نماید. **تنظیم مهرهای زمانی به صورت پیشفرض معتبر و عدم امکان دستکاری غیرمجاز)**	
۴	**امکان بروزرسانی**
محصول امکان به‌روزرسانی نرم افزار و میان افزار محصول را برای مدیر سیستم فراهم می نماید.	

تخصیص منابع

۱	**صحت کارکرد**
محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکردکارکردهای اصلی محصول اطمینان حاصل نماید.	

دسترسی به محصول

۱	**محدودیت بر روی چندین نشست همزمان**
محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	
۲	**قفل کردن و خاتمه دادن به نشست ها**
محصول باید کلیه نشست‌های تعاملی راه‌دور[1] را پس از مدت زمانی که غیرفعال هستند و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.	
۳	**قفل کردن و خاتمه دادن به نشست ها**
محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	
۴	**سوابق دسترسی به محصول**
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس روز و زمان است.	
۵	**سوابق دسترسی به محصول**
در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس روز و زمان و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز است.	
۶	**سوابق دسترسی به محصول**
محصول نمی تواند اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.	
۷	**محدودیت بر روی چندین نشست همزمان**
محصول توانایی ممانعت از ایجاد نشست بر اساس پارامتر مکان را دارد.	

کانال‌ها/مسیرهای مورد اعتماد

۱	**کانال امن ۱**
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 داده و از تغییر و افشاء داده تبادلی حفاظت نموده و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام **Error! Reference source not found.** و در صورت انتخاب TLS، رعایت الزامات	

[1] Remote

Error! Reference source not found. تا **Error! Reference source not found.** که در بخش **Error! Reference source not found.** بیان گردیده است، الزامی است.	
۲	**کانال امن ۲۱**
محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.	
۳	**کانال امن ۳**
محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.	

الزامات تضمین امنیت

[این بخش از سند پروفایل حفاظتی کپی گردد.]

خلاصه مشخصات محصول [در این بخش به ازای هریک از کلاس‌های کارکردی در فصل پنجم، خلاصه‌ای از عملکرد امنیتی در آن کلاس بیان گردد.]

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 RSA با اندازه کلید ۲۰۴۸ بیت یا بیشتر که از اسناد FIPS PUB ۱۸۶-۴، "Digital Signature Standard (DSS)"، "Appendix B. 3.پیروی میکند تولید کنند و رمزنگاری و رمزگشایی را مطابق با
الگوریتم رمزنگاری متقارن AES Key Wrap with Paddi ng (KWP مطابق سند NIST SP 38-800 F ، با 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 مشخصههای امنیتی شناسه کاربر داده های احراز هویت، نقش کاربر، وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)، IPکاربر، 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.
oزمانیکه 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 TLS, HTTPS میان خود و موجودیتIT

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