به نام خدا

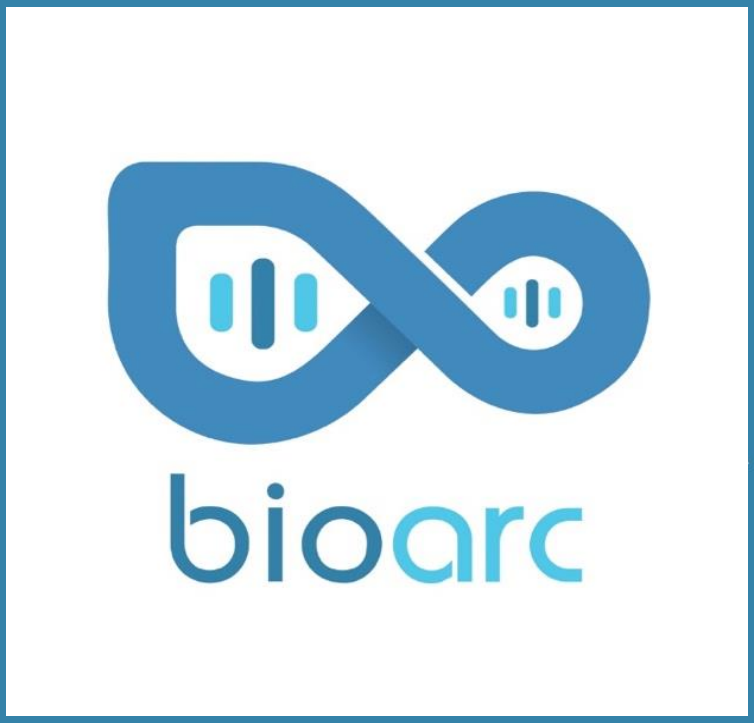
سند هدف امنیتی

[بایوآرک-نسخه ۱.۰]

[شرکت زیست داده پرداز آرکا]

[مرداد ۱۴۰۳]

[نسخه ۱.۰]


bioarc

فهرست

۱ معرفی

خواستگاه بایوآرک دانشگاه است. بایوآرک حاصل همکاری اساتید دانشگاه علوم پزشکی تهران و فارغ‌التحصیلان گروه کامپیوتر دانشگاه صنعتی شریف است که در گروه کامپیوتر دانشگاه ایلام شکل گرفته است. همکاری این دو مرکز در سال ۲۰۱۶ با توجه به نیاز مرکز تحقیقات روماتولوژی دانشگاه علوم پزشکی تهران به راه‌اندازی یک سامانه جامع برای ثبت اطلاعات بیماران روماتیسمی آغاز شد. پس از گذشت دو سال از آغاز به کار سامانه جامع نظام ثبت بیماران و به روز رسانی برنامه در مرکز تحقیقات روماتولوژی تصمیم گرفته شد که سایر مراکز تحقیقاتی کشور از این سامانه جامع و قدرتمند بهره‌مند شوند. بر این اساس پلتفرم دانش‌بنیان سامانه جامع نظام ثبت بیماران بایوآرک کار خود را از سال ۲۰۱۹ به طور رسمی آغاز کرد. طی یک سال اخیر علاوه بر مرکز تحقیقات روماتولوژی مراکز بزرگ تحقیقاتی کشور مانند پژوهشگاه غدد و متابولیسم، مرکز تحقیقات ایمونولوژی، آسم و آلرژی، مرکز تحقیقات بیماری مزمن کلیوی، مرکز تحقیقات بیماری‌های تاولی پوست، مرکز تحقیقات بیماری‌های کلیوی و مجاری ادراری و ... از این پلتفرم برای ثبت اطلاعات بیماران استفاده کرده‌اند. با توجه به استقبال مراکز تحقیقاتی از سامانه جامع نظام ثبت بیماران، بایوآرک تصمیم به راه‌اندازی یک برنامه جامع بر پایه مسائل علمی پزشکی جهت استفاده در مطب های خصوصی پزشکان گرفت. این برنامه کاملا تخصص محور بوده و علاوه بر مدیریت قدرتمند مطب حاوی اطلاعات علمی در زمینه تخصص‌های مختلف پزشکی است. این برنامه با همکاری و مشاوره بیش از ۵۰ نفر از اساتید دانشگاه علوم پزشکی تهران و سایر دانشگاه‌های کشور تهیه شده است. هدف اصلی بایوآرک تاثیرگزاری و تغییر در جامعه به ویژه جامعه پزشکی می‌باشد. بایوآرک می‌کوشد با تکیه بر مسائل علمی و پشتیبانی قوی تاثیر عمیق و ژرفی در ثبت اطلاعات بیماران و ایجاد پرونده الکترونیک در کشور داشته باشد.

۱.۱ مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه هوشمند اطلاعات بیمارستانی بایوآرک
نسخه	۱.۰
تاریخ	مرداد ۱۴۰۳
نویسندگان	گروه توسعه شرکت زیست داده پرداز آرکا

نام شرکت	زیست داده پرداز آرکا
نام محصول	بایوآرک
نوع محصول	برنامه کاربردی تحت وب

نسخه‌ی محصول	۱.۰

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**
پردازنده	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
فضای آزاد دیسک	DDR4 HDD: 926G NVME NVME OS: Centos Stream 9
حافظه	128G
سیستم عامل	Linux
DBMS	MariaDB 11.3.2
سرور وب	
مرورگر	-
Web installer	-
سایر نرم افزارها	
سایر الزامات نیازمندی ها	-IP: 1 Valid IP -دارا بودن ارتباط اینترانت جهت تبادل داده با تامین، سلامت، ساخد، دیتاس و سپاس -گواهی SSL برای دامنه مد نظر -letsencrypt -عدم استفاده از ssl offloading روی دامنه -اختصاص آی‌پی اینترانت به سرور و باز بودن پورت‌های ۴۴۳ و ۸۰ رو این آی‌پی -اختصاص فضای بک‌اپ جهت ذخیره بک‌آپ‌های ساعتی (حداقل فضای ۱۰۰ گیگ) -اخذ نام کاربری دیتاس

۲ ادعای انطباق

۱.۲ 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

۲.۲ شرح محصول

سامانه هوشمند اطلاعات مدیریتی بیمارستان بایوآرک به منظور رسیدن به اهداف زیر تولید شده است: پائین آوردن زمان پذیرش، زمان ترخیص، زمان انتقال بیمار، زمان نسخه نویسی و درخواست های پاراکلینیکی، زمان اخذ جواب ها، زمان مراجعه به اطلاعات قبلی پرونده، بالا بردن میزان دقت در درج اطلاعات و درخواست ها که در حالت دستی ناخوانا و ... هست، تسریع ارتباطات بین بخشی، افزایش دقت و تسریع در ارائه خدمات به بیمار، بازیابی سریع پرونده برای اهداف گوناگون و در نهایت بالابردن میزان رضایت بیمار، ارائه خدمات بهتر، دریافت آمار و گزارشات روزانه و زمانی، اطلاع از وضعیت درآمد و هزینه بیمارستان، تسریع در تشکیل و گردش پرونده در بیمارستان، و ... . در زیر به چند مورد از مزایای سامانه بایوآرک اشاره می شود:

- سامانه بایوآرک مبتنی بر وب می‌باشد. بنابراین ویروسی شدن کامپیوترها هیچگونه تاثیری بر روی امنیت سامانه و اطلاعات موجود در آن ندارد.
- در نرم‌افزارهای تحت وب (که سامانه جامع پزشکی فرانور از این نوع می‌باشد)؛ بروزرسانی نرم‌افزار ارتباطی با امنیت داده‌ها و اطلاعات ندارد و صرفا جهت بهبود فرآیندهای کسب و کار انجام می‌شود. سامانه بایوآرک به صورت نامحسوس و به طور خودکار بروز می‌شود. علاوه براین، توسعه دهندگان نرم‌افزار به جای نصب نسخه جدید به صورت جداگانه در چندین دستگاه، تنها نیاز به ارائه یک نسخه به روز شده از برنامه دارند. کاربران نیز بدون هیچ تداخل و یا اتلاف زمانی می‌توانند روی موضوعات اصلی کسب و کارشان تمرکز کنند.
- در نوشتن سامانه بایوآرک از زبان برنامه‌نویسی PHP که یک زبان برنامه‌نویسی منبع باز (Open Source) می‌باشد، استفاده شده است. زبان برنامه‌نویسی PHP به علت Open Source بودن و پذیرش در تمام جوامع بین الملل و عدم نیاز به کرک نمودن، شامل محدودیت‌ها و مشکلات امنیتی و اطلاعاتی نشده و عملکرد با ثباتی را در Backend و دیتابیس ارائه می‌دهد. همچنین به علت Open Source بودن زبان

برنامه‌نویسی PHP ، استفاده از آن با هیچ یک از قوانین بین المللی از جمله کپی رایت تناقض نداشته و سامانه جامع پزشکی فرانور قابلیت پیاده‌سازی در تمام مراکز بهداشتی-درمانی خارج از کشور را نیز دارد.

- زبان برنامه‌نویسی PHP سامانه بایوآرک بسیار انعطاف‌پذیر بوده و به تبع آن، سامانه جامع فرانور نیز قابلیت Customization بسیار بالایی داشته باشد.
- یکی دیگر از مزیت هایی که در استقرار و اجرای سامانه بایوآرک که با زبان برنامه‌نویسی PHP نوشته شده، این است که این زبان وابسته به هیچ Platform خاصی نیست و می‌توان آن را بر روی هر سیستمی عاملی (اعم از ویندوز، مکینتاش، لینوکس و ..) اجرا و استفاده کرد.
- حفاظت از اطلاعات هر یوزر – دادن امتیاز دسترسی و تعریف حقوق دسترسی هر یوزر، کاربران را از هرگونه دسترسی غیرمجاز به اطلاعاتشان حفاظت می کند.
- محدود کردن شبکه – لینک و آدرس دسترسی به سامانه دارای محدوه مجاز دامنه ای می باشد و قابلیت تعریف به عنوان شبکه اینترانت را دارد. بنابراین از هرجایی نمی توان به آدرس سامانه دسترسی داشت.
- ممیزی امنیتی – سیستم دارای پروتکل های مختلفی جهت ورود هر کاربر می باشد. دارای کد امنیتی نیز می باشد تا ربات ها و بدافزارها امکان ورود به سامانه را نداشته باشند.
- شناسایی و احراز هویت – کاربران مجاز بعد از اینکه با نام کاربری و رمز عبور مخصوص خود به سامانه وارد شدند، می توانند به قسمت ها و عملکردهایی از سامانه که در تنظیمات نقش ها و دسترسی های مجاز برای هریک از آن ها تعریف شده است، دسترسی داشته باشند.
- لاگ ورود کاربران - لاگ ورود تمام کاربران در سیستم ثبت می شود و قابل ردیابی و پیگیری می باشد.
- مدیریت امنیت سامانه –می توان نقش ها و دسترسی های هریک از نقش ها را ویرایش یا حذف نمود. همچنین می توان رمز کاربری هریک از کاربران را ریست کرد به منظور تعریف روز جدید. می توان تاریخ انقضا برای زمان محدود دسترسی کاربر به سامانه تعریف نمود و بعد آن زمان دسترسی کاربر به سامانه به طور اتومات قطع شود.

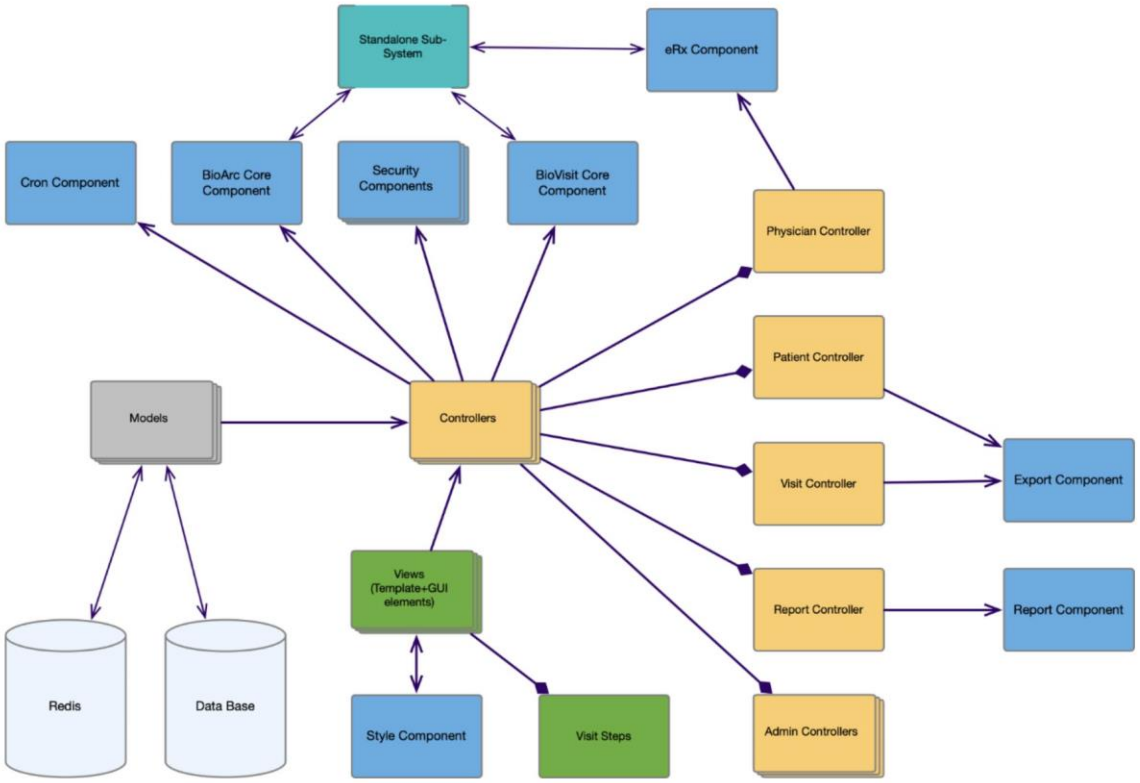
شعار اصلی مجموعه بایوآرک، Altogether است؛ که به معنای پوشش دادن تمام نیازهای موجود در یک بیمارستان از جنبه‌های مختلف می باشد. در سامانه HIS بایوآرک، هدف ما در ابتدا راه اندازی نرم‌افزار در تمام بیمارستان‌های داخل کشور و سپس تبدیل شدن به یک برند برتر منطقه‌ای می‌باشد.

۱.۲.۲ حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
لیستی از تمام سخت افزار	-
لیستی از تمام میان افزار	-
لیستی از تمام نرم افزار	PHP-FPM 8.12, Redis 7.2, Mariadb 11.3, NGINX 1.26, monit, Bind
نحوه ارتباط با دیتابیس	از طریق unixsocket
نحوه ارتباط با شبکه	از طریق پورت ۸۰ و ۴۴۳
و سایر بخش های راهنمایی که تشکیل دهنده هدف ارزیابی هستند	-

در قسمت زیر، قرار گیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شده است.



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

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 امنیتی	تاکید منطقی این مورد بر این موضوع است که ببینیم کدام کاربران آنلاین و در حال کار با سیستم می باشند و همچنین کدام تراکنش ها در حال اجرا شدن می باشد. این محصول ارزیابی توابع مدیریتی متعددی برای تضمین کارآمدی و مدیریت امن محصول را داراست. این محصول با مکانیسم های کنترل دسترسی مبتنی بر قوانین، تضمین می نماید که توابع تنها در اختیار افرادی هستند که مجوز دسترسی دارند.

	سرپرست سامانه توانایی ایجاد قوانین کاربر و تعیین افراد مجاز برای دسترسی به توابع مشخص را داراست. عملکرد امنیتی سامانه، لاگ های احراز هویت که شامل رخدادهای قابل ردیابی و ممیزی است را تولید می کند. همچنین تاریخ و زمان رویدادها، نام های کاربری و رخدادهایی که توسط کاربران مجاز حادث شده اند، ثبت و ضبط می شود.
حفاظت از امنیت اطلاعات کاربران	ادمین های مجاز سیستم قادر به اعمال موارد زیر بر روی حساب کاربری کاربران می باشند: -دسترسی به اضافه و کم کردن نقش ها و دسترسی های هر کاربر -باز کردن یا قفل کردن حساب کاربری کاربران مجاز -ریست کردن یا تغییر رمز عبور حساب کاربری
شناسایی و احراز هویت	شناسایی و احراز هویت شفاف کاربران و همچنین شناسایی کاربران مجاز از غیرمجاز و همچنین اختصاص درست ویژگی های امنیتی به کاربران و حقوق دسترسی آن ها، از جمله الزامات مهم برای حصول اطمینان از پیاده سازی سیاست های امنیتی موردنظر می باشد. پیش از صدور مجوز برای هرگونه جریان اطلاعاتی، تمامی کاربران بایستی شناسایی و احراز هویت شوند. بدین منظور، محصول مورد ارزیابی، اعتبار اعلامی توسط کاربر را با اطلاعات هویتی ذخیره شده در پایگاه داده بررسی می نماید.
کنترل دسترسی	توابع کنترل دسترسی تنها زمانی به کاربر اجازه دسترسی به منابع حفاظت شده را می دهد که شناسه کاربر یا قوانین تعریف شده برای کاربر، مجوز اعمال عملیات خواسته شده در آن منبع را صادر کرده باشد. قوانین دسترسی در فهرست های کنترل دسترسی مرتبط با هر شیء ذخیره می گردد.
رویداد نگاری	مشاهده تمامی فعالیت های انجام شده توسط کاربران

۳ مسائل امنیتی

۱.۳ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم میتواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم می تواند 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 می تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده های می توانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می تواند با دسترسی به داده ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردها، مستندات و داده های حفاظت شده توسط محصول می تواند بدون مجوز تغییر یابند. مهاجم می تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می تواند 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 می دهد که صحت رکوردها و مستندات تضمین شده نمی باشد. 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 می تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می باشد 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

تهدیدات	توضیحات
	می تواند 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 می شوند، می تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می تواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواست های بسیار در یک بازه زمانی کوتاه صورت می گیرد؛ طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده ای از حمله شامل ارسال درخواست های بسیار از یک رنج IP مشخص می باشد که به نام حمله DoS شناخته می شود. نوع دیگر پیشرفته تر حمله DDoS می باشد که از BOTNET استفاده می نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده های ورودی مخرب	مهاجم می تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم می تواند به داده کاربر خاص دسترسی پیدا نماید، 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 نماید.

۲.۳ 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 می گیرند.
ارتباطات امن مبتنی بر TLS	تمام کانال های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده 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 پیش فرض و صفحات ۴۰۴ ، مقادیر احراز هویت پیش فرض، نام کاربری پیش فرض، پورت های پیش فرض، صفحات پیش فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می نمایند. این خط مشی سازمانی بسیار مهم است؛ به خصوص زمانی که محصول یا هر مولفه 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.

۳.۳ فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال می نمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می نمایند.

فرضیات	توضیحات
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ می نمایند.
محیط امن	فرض شده است که تمام پیشبینی های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که ساز و کاری 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 می گیرد.
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 نمی رود. همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی دهد.
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 در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می شوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می گیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می شود.

۴ اهداف امنیتی

۱.۴ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش 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 می نماید. 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 احراز هویت نماید. از جمله سازوکارها می توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت براساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش ها 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 می تواند بیانگر حمله DoS باشد. محصول باید برای

هدف امنیتی	توضیحات
	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 واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش ها و مجوزهایی تنظیم 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 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 داده ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می گردد.

۲.۴ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام 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 می توان به غیرفعال نمودن سرویس ها، پورت ها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله ای لازم برای تمام آسیب پذیری های امنیتی شناخته شده را در نظر می گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه های غیر از محصول نیز مورد ممیزی قرار می گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می باشد. 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.

هدف امنیتی	توضیحات
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.

۵ الزامات کارکرد امنیتی

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

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	تولید داده ممیزی ۳	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 ۳	FAU_SAR.2.1
۷	بازبینی داده ممیزی ۴	FAU_SAR.3.1
۸	ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۹	ذخیره سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۱۰	ذخیره سازی رویدادهای ممیزی ۷	FAU_STG.4.1
۱۱	انتخاب داده ممیزی ۱	FAU_SEL.1.1
۱۲	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۱۳	عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱ (۱)	FCS_COP.1.1(1)
۱۴	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۵	مدیریت کلمه عبور	FIA_PMG_EXT.1.1
۱۶	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۷	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸	تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۱۹	شناسایی کاربر ۱	FIA_UID.1.1
۲۰	احراز هویت کاربر ۱	FIA_UAU.1.1
۲۱	احراز هویت کاربر ۲	FIA_UAU.1.2
۲۲	احرازهویت کاربر ۷	FIA_UAU.5.1
۲۳	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۲۴	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۲۵	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۲۶	ورود داده های کاربری به محصول ۴	FDP_ITC.2.1
۲۷	ورود داده های کاربری به محصول ۵	FDP_ITC.2.2
۲۸	ورود داده های کاربری به محصول ۶	FDP_ITC.2.3
۲۹	خروج داده های کاربری از محصول ۳	FDP_ETC.2.1
۳۰	صحت داده های کاربری ذخیره شده ۲	FDP_SDI.2.1
۳۱	صحت داده های کاربری ذخیره شده ۳	FDP_SDI.2.2
۳۲	خط مشی کنترل دسترسی ۱	FDP_ACC.1.1
۳۳	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۳۴	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۳۵	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۳۶	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۳۷	مدیریت مشخصه های امنیتی ۱	FMT_MSA.1.1
۳۸	مدیریت مشخصه های امنیتی ۳	FMT_MSA.3.1
۳۹	مدیریت مشخصه های امنیتی ۴	FMT_MSA.3.2
۴۰	مدیریت داده های محصول ۱-مدیر سیستم	FMT_MTD.1.1(1)

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۱	مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده	FMT_MTD.1.1(2)
۴۲	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۴۳	نقش های امنیتی ۱	FMT_SMR.1.1
۴۴	نقش های امنیتی ۲	FMT_SMR.1.2
۴۵	لغو مشخصه های امنیتی ۱	FMT_REV.1.1
۴۶	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۴۷	سازگاری داده های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۴۸	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۴۹	مهرهای زمانی ۱	FPT_STM.1.1
۵۰	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۵۱	محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
۵۲	قفل کردن و خاتمه دادن به نشست ها ۵	FTA_SSL.3.1
۵۳	قفل کردن و خاتمه دادن به نشست ها ۶	FTA_SSL.4.1
۵۴	سوابق دسترسی به محصول ۱	FTA_TAH.1.1
۵۵	کانال امن ۱	FTP_ITC.1.1
۵۶	کانال امن ۲	FTP_ITC.1.2
۵۷	کانال امن ۳	FTP_ITC.1.3
۵۸	مسیر امن ۱	FTP_TRP.1.1
۵۹	مسیر امن ۲	FTP_TRP.1.2
۶۰	مسیر امن ۳	FTP_TRP.1.3
۶۱	به روز رسانی امن ۲	FPT_TUD_EXT.1.2
۶۲	به روز رسانی امن ۳	FPT_TUD_EXT.1.3
الزامات مربوط به پیوست اول		
۶۳	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۶۴	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۵	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۶۶	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۶۷	الزامات پروتکل IPSEC (۲)	FCS _IPSEC_EXT.1.2
۶۸	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۶۹	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۷۰	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۷۱	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۷۲	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۷۳	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۷۴	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۷۵	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۷۶	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۷۷	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۷۸	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۷۹	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۸۰	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۸۱	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۸۲	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۸۳	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۸۴	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۸۵	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۸۶	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۸۷	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۸۸	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۸۹	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۹۰	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۹۱	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3

شماره الزام	نام الزام	تطابق الزام با استاندارد
۹۲	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۹۳	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۹۴	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۹۵	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۹۶	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۹۷	الزامات پروتکل TLS Client / احراز هویت ۱	FCS_TLSC_EXT.1.1
۹۸	الزامات پروتکل TLS Client / احراز هویت ۲	FCS_TLSC_EXT.1.2
۹۹	الزامات پروتکل TLS Client / احراز هویت ۳	FCS_TLSC_EXT.1.3
۱۰۰	الزامات پروتکل TLS Client / احراز هویت ۴	FCS_TLSC_EXT.1.4
۱۰۱	الزامات پروتکل TLS Client / احراز هویت دوطرفه ۱	FCS_TLSC_EXT.2.1
۱۰۲	الزامات پروتکل TLS Client / احراز هویت دوطرفه ۲	FCS_TLSC_EXT.2.2
۱۰۳	الزامات پروتکل TLS Client / احراز هویت دوطرفه ۳	FCS_TLSC_EXT.2.3
۱۰۴	الزامات پروتکل TLS Client / احراز هویت دوطرفه ۴	FCS_TLSC_EXT.2.4
۱۰۵	الزامات پروتکل TLS Client / احراز هویت دوطرفه ۵	FCS_TLSC_EXT.2.5
۱۰۶	الزامات پروتکل TLS Server / احراز هویت ۱	FCS_TLSS_EXT.1.1
۱۰۷	الزامات پروتکل TLS Server / احراز هویت ۲	FCS_TLSS_EXT.1.2
۱۰۸	الزامات پروتکل TLS Server / احراز هویت ۳	FCS_TLSS_EXT.1.3
۱۰۹	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۱۰	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۲	FCS_TLSS_EXT.2.2
۱۱۱	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۳	FCS_TLSS_EXT.2.3
۱۱۲	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۴	FCS_TLSS_EXT.2.4
۱۱۳	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۵	FCS_TLSS_EXT.2.5
۱۱۴	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۶	FCS_TLSS_EXT.2.6
۱۱۵	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۱۱۶	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۱۱۷	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۱۱۸	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱۹	الزامات پروتکل X509 (۵)	FIA_X509_EXT.3.1
۱۲۰	الزامات پروتکل X509 (۶)	FIA_X509_EXT.3.2

۱.۵ کلاس ممیزی امنیت

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

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

- ورود و خروج کاربر به / از سیستم
- رویدادهای قابل ممیزی (این رویدادها در جدول زیر آمده است):

مولفه	رویداد قابل ممیزی	جزئیات
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی	
بازبینی داده ممیزی ۳	تلاش های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی	
ذخیره سازی رویدادهای ممیزی ۷	عملیات انجام شده به دلیل شکست ذخیره سازی ممیزی	به دلیل ذخیره سازی داده های ممیزی در پایگاه داده بروز چنین مشکلی امکان پذیر نمی باشد. یعنی اگر احتمال بروز چنین آسیب پذیری وجود داشت، یعنی تنظیمات پایگاه داده درست ست نشده که در این صورت به طور کلی نرم افزار اجرا نخواهد شد.

عملیات کنترل دسترسی ۱	تمامی درخواست های ناموفق برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	
مدیریت کلمه عبور	تلاش موفق و ناموفق ورود کاربر	تمامی درخواست های ورود اعم از موفق یا نا موفق در سیستم ثبت می گردد.
مدیریت مشخصه های امنیتی ۱	تمامی تغییرات بر روی مقادیر مشخصه های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد
مدیریت داده های محصول ۱ - مدیر سیستم	تمامی تغییرات بر روی مقادیر داده های امنیتی	
مدیریت داده های محصول ۱ - کاربرعادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده های امنیتی	تمامی فعالیت ها در داده های ممیزی ثبت می گردد.
تغییرات روی موجودیت های غیر فعال	افزودن،ویرایش،حذف موجودیت های غیر فعال	
تغییرات روی موجودیت های فعال	افزودن،ویرایش،حذف موجودیت های فعال	
تعلیق ورود موجودیت فعال	جلوگیری از ورود کاربر پس از ۴ بار تلاش ورود ناموفق	

شماره الزام	نام الزام
۲	**تولید داده ممیزی ۲**

محصول می تواند برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

- تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد

- نوع کاربری، IP کاربر، محل خدمت کاربر

شماره الزام	نام الزام
۳	**تولید داده ممیزی ۳**
برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول می تواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید	

شماره الزام	نام الزام
۴	**بازبینی داده ممیزی ۱**
محصول می تواند امکان 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 فراهم نماید.	

شماره الزام	نام الزام
۵	**بازبینی داده ممیزی ۲**
محصول می تواند رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر نمایش دهد.	

شماره الزام	نام الزام
۶	**بازبینی داده ممیزی ۳**
محصول می تواند از دسترسی کلیه کاربران به جز کاربرانی که به آنها مجوز دسترسی خواندن داده شده باشد (الزام شماره ۴) جهت خواندن رکوردهای ممیزی ممانعت نماید.	

شماره الزام	نام الزام
۷	**بازبینی داده ممیزی ۴**
محصول می تواند 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.	

شماره الزام	نام الزام
۸	**ذخیره سازی رویدادهای ممیزی ۱**
محصول می تواند رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت 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.	

شماره الزام	نام الزام
۹	**ذخیره سازی رویدادهای ممیزی ۲**
محصول قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در محل ذخیره سازی آنها می باشد.	

شماره الزام	نام الزام
۱۰	**ذخیره سازی رویدادهای ممیزی ۷**
محصول در صورت پر شدن محل ذخیره سازی رکورد ممیزی «از ذخیره رویدادهای قابل ممیزی، بجز آنهایی که توسط مدیر سیستم تعیین می گردد، جلوگیری نماید و هشدار لازم را با استفاده از پیام کوتاه، مدیر سیستم را مطلع نماید».	

شماره الزام	نام الزام
۱۱	**انتخاب داده ممیزی ۱**
محصول می تواند قادر به انتخاب مجموعه ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه های زیر باشد: • هویت موجودیت فعال، نوع رخداد (عملیات) • گروه کاربری • محدوده زمانی	

- موضوع، فرم، IP

۲.۵ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۲	**تولید کلید رمزنگاری ۱**
محصول می تواند کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتمهای تولید کلید استاندارد زیر تولید کنند. استفاده از طرح RSA با اندازه کلید ۲۰۴۸ بیت یا بیشتر که از این اسناد پیروی می کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)، Appendix B.3	

شماره الزام	نام الزام
۱۳	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱ (۱)**
محصول می تواند رمزنگاری و رمزگشایی را مطابق با الگوریتم رمزنگاری متقارن AES Key Wrap with Paddi ng (KWP مطابق سند NIST SP 800-38F ، با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.	

شماره الزام	نام الزام
۱۴	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی می تواند خدمات امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم رمزنگاری زیر ارائه کند: الگوی RSA : اندازه کلیدهای ۲۰۴۸ بیتی و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال DSS »بخش ۴	

۳.۵ کلاس شناسایی و احرازهویت

شماره الزام	نام الزام
۱۵	**مدیریت کلمه عبور**
محصول می تواند قابلیت های مدیریت رمزعبور را که در زیر ذکر شده اند برای رمزهای عبور مدیریتی فراهم نماید: ۱-رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص"!"، "@"، "#"، "$"، "٪"، "*"، "("، ")"، "_"، "+"، "^"، "&"، "{"، "}"، ":"، ";"، "?"، "."، "." باشند. ۲-حداقل طول رمزعبور باید توسط مدیر امنیت، قابل تنظیم باشد	

شماره الزام	نام الزام
۱۶	**مدیریت احراز هویت ناموفق ۱**
محصول می تواند با استفاده از یک عدد مثبت قابل تنظیم از طرف مدیر سیستم تعداد تلاش های احراز هویت ناموفق را مدیریت نماید.	

شماره الزام	نام الزام
۱۷	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاشهای ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید و یا از آن بیشتر شد، محصول می تواند عملیات "جلوگیری از ورود کاربر به مدت تعیین شده توسط مدیر" اجرا نماید که باعث پیچیده تر کردن عمل احراز هویت مجدد کاربر شود.	

شماره الزام	نام الزام
۱۸	**تعریف مشخصات کاربر ۱**

محصول باید مشخصه های امنیتی زیر را برای هر کاربر نگهداری نماید:

- شناسه کاربر داده های احراز هویت
- نقش کاربر
- وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)
- IP کاربر
- رمز عبور کاربر

شماره الزام	نام الزام
۱۹	**شناسایی کاربر ۱**

محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد:

- مشاوره راهنمای نحوه ورود به سیستم

شماره الزام	نام الزام
۲۰	**احراز هویت کاربر ۱**

محصول می تواند پیش از احراز هویت کاربر، اجازه اقدامات زیر را به کاربر دهد:

- بازیابی رمز عبور

شماره الزام	نام الزام
۲۱	**احراز هویت کاربر ۲**
محصول می تواند هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نماید.	

شماره الزام	نام الزام
۲۲	**احراز هویت کاربر ۷**
محصول باید اقدامات زیر را برای احرازهویت کاربر فراهم آورد: • نام کاربری و کلمه عبور • احراز هویت از طریق Active Directory	

شماره الزام	نام الزام
۲۳	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۱**
محصول می تواند مشخصه های امنیتی زیر را برای کاربر فعال نگهداری نماید: • شناسه کاربر • نقشهای 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)

شماره الزام	نام الزام
۲۴	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲**

محصول می تواند قوانین زیر را بر روی اتصال اولیه کاربر فعال اعمال نماید:

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

شماره الزام	نام الزام
۲۵	**انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۴**

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

- هیچ تغییری در طول نشست فعال مجاز نمی باشد.

۴.۵ کلاس حفاظت از داده های کاربری

شماره الزام	نام الزام
۲۶	**ورود داده های کاربری به محصول ۴**

شماره الزام	نام الزام
محصول هنگام دریافت داده کاربری، خط مشی کنترل دسترسی، فرمت های مجاز داده ها (jpg,docx) را اعمال می نماید.	

شماره الزام	نام الزام
۲۷	**ورود داده های کاربری به محصول ۵**
محصول می تواند از مشخصه های امنیتی مرتبط با داده های کاربری را هنگام ورود داده ها استفاده نماید.	

شماره الزام	نام الزام
۲۸	**ورود داده های کاربری به محصول ۶**
محصول می تواند اطمینان دهد که پروتکل مورد استفاده برای انتقال، ارتباط و همبستگی بین مشخصه های امنیتی و داده کاربری دریافت شده را فراهم مینماید	

شماره الزام	نام الزام
۲۹	**خروج داده های کاربری از محصول ۳**
محصول می تواند 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.	

شماره الزام	نام الزام

شماره الزام	نام الزام
۳۰	**صحت داده های کاربری ذخیره شده ۲**
محصول می تواند داده کاربری حساس ذخیره شده در مکان تحت کنترل خود را براساس مشخصه های رمزنگاری امن نگهداری کرده و به منظور شناسایی خطای صحت داده رکورد و داده ممیزی، پایش نماید.	

شماره الزام	نام الزام
۳۱	**صحت داده های کاربری ذخیره شده ۳**
هنگام تشخیص خطای صحت داده، محصول می تواند ثبت ممیزی را صورت دهد.	

شماره الزام	نام الزام
۳۲	**صحت داده های کاربری ذخیره شده ۲**

محصول می تواند دسترسی بر اساس نوع کاربری که هنگام ورود کاربر شناسایی می شود را بر روی موارد زیر اعمال نماید:

- موجودیت های فعال به تفکیک ماژول های سیستم
  - نرم افزار مدیریت اموزش
    - مدیر سیستم
    - مدیر استانی

شماره الزام	نام الزام

- نرم افزار سامانه فراگیر
  - فراگیر
  - مدرس
- نرم افزار یادگیری الکترونیکی
  - مدیر سیستم
  - فراگیر
  - مدرس

- موجودیت غیرفعال:
  - رکوردها، مستندات
  - داده های متعلق به کاربر
  - داده احراز هویت
  - داده با این معیارها: عکس کاربر با فرمت های BMP, PNG, JPG,GIF
  - کلاس های آموزشی
  - دوره های آموزشی
- عملیات:
  - ایجاد موجودیت غیرفعال جدید
  - انتقال موجودیت غیرفعال
  - ویرایش و حذف موجودیت غیر فعال
  - ایجاد موجودیت فعال جدید

شماره الزام	نام الزام
	○ انتقال موجودیت فعال ○ ویرایش و حذف موجودیت فعال ○ تغییر دسترسی ها به موجودیت غیرفعال ○ عملیات بر روی فراداده های وابسته به موجودیت غیرفعال

شماره الزام	نام الزام
۳۳	**عملیات کنترل دسترسی ۱**
محصول می تواند سطح دسترسی را با توجه به موارد زیر بر روی موجودی تهای غیرفعال اعمال نماید: • هویت کاربر • نقش ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند	

شماره الزام	نام الزام
۳۴	**عملیات کنترل دسترسی ۲**
محصول می تواند قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نمایند: عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با	

شماره الزام	نام الزام
	شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.

شماره الزام	نام الزام
۳۵	**عملیات کنترل دسترسی ۳**
محصول می تواند براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه شده توسط محصول دسترسی دارند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.	

۵.۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۳۶	**مدیریت کارکرد در محصول ۱**
محصول می تواند توانایی تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار عملکرد تمام عملکردهای مدیریت امنیت سیستم را به مدیر سیستم محدود نماید.	

شماره الزام	نام الزام
۳۷	**مدیریت مشخصه های امنیتی ۱**

شماره الزام	نام الزام
محصول می تواند 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 نماید.	

شماره الزام	نام الزام
۳۸	**مدیریت مشخصه های امنیتی ۳**
محصول برای مشخصه های امنیتی که برای اعمال خط مشی استفاده می شوند، می تواند مقادیر پیش فرض محدود شده ای درنظر بگیرد.	

شماره الزام	نام الزام
۳۹	**مدیریت مشخصه های امنیتی ۴**
محصول برای تعیین مقادیر اولیه پیشنهادی می تواند به مدیر سیستم اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش فرض را لغو و تغییر دهد.	

شماره الزام	نام الزام
۴۰	**مدیریت داده های محصول ۱-مدیر سیستم**

شماره الزام	نام الزام
محصول می تواند توانایی تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم محدود نماید.	

شماره الزام	نام الزام
۴۱	**مدیریت داده های محصول ۱-کاربر عادی، وارد کننده داده**
محصول می تواند توانایی تغییر پیش فرض، پرس و جو، تغییر پسورد به کاربر عادی محدود نماید.	

شماره الزام	نام الزام
۴۲	**کارکردهای مدیریتی محصول ۱**

محصول می تواند قادر به انجام کارکردهای مدیریتی زیر باشد:

مولفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ ویرایش رویدادهای ممیزی
ذخیره سازی رویدادهای ممیزی ۷	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
عملیات کنترل دسترسی ۱	مدیریت مشخصه های مورد استفاده برای ایجاد دسترسی و یا منع

شماره الزام	نام الزام	
۴	ورود داده های کاربری به محصول	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
۲	صحت داده های کاربری ذخیره شده	عملیاتی برای تشخیص یک خطای صحت داده که می تواند قابل پیکربندی باشد.
۱	مدیریت احراز هویت ناموفق	• مدیریت حد آستانه برای تلاشهای ناموفق. • مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.
۱	تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد.
	مدیریت کلمه عبور	مدیریت معیارها برای بررسی کلمه عبورها.
۱	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز می تواند مقادیر مشخصه های امنیتی موجودیت های فعال پیش فرض را تعریف و یا تغییر دهد.
۱	مدیریت مشخصه های امنیتی	مدیریت گروهی از نقش هایی که با مشخصه های امنیتی در تعامل هستند.
۳	مدیریت مشخصه های امنیتی	• مدیریت گروهی از نقش هایی که مقادیر اولیه را مشخص می کنند. • نقش مدیر سیستم توانایی مشخص نمودن مقادیر اولیه را داراست.

شماره الزام	نام الزام	
		• مدیریت مقادیر پیش فرض برای کنترل دسترسی محصول
مدیریت داده های محصول ۱-مدیر سیستم		مدیریت گروهی از قوانین مرتبط با داده های محصول
مدیریت داده های محصول ۱-کاربرعادی، وارد کننده داده		مدیریت گروهی از قوانین مرتبط با داده های محصول **توضیح**: کاربر عادی نمی تواند قوانین مرتبط با داده های محصول را مدیریت کند. چون در فرآیند آموزش کاربر عادی نباید این امکان را داشته باشد.
نقش های امنیتی ۱		مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند
محدودیت بر روی چندین نشست همزمان ۱		مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر. **توضیح**: در ماژول یادگیری الکترونیکی با توجه به اینکه نشست های همزمان یک کاربر در آن واحد ممکن است موجب سوء استفاده گردد، نشست های فعال کاربر محدود به یک نشست می باشد؛ اما با توجه به ماهیت کسب و کار سایر ماژول ها این مکانیسم حساسیت برانگیز نمی باشد.
قفل کردن و خاتمه دادن به نشست ها		• تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد.

شماره الزام	نام الزام
	• تعیین زمان پیش فرض غیرفعال بودن کاربر که نشست خاتمه یابد.

شماره الزام	نام الزام
۴۳	**نقش های امنیتی ۱**

نقش های زیر در محصول باید تعریف شده باشد:

- نرم افزار مدیریت اموزش
  - مدیر سیستم
- نرم افزار یادگیری الکترونیکی
  - مدیر سیستم
  - فراگیر
  - مدرس

شماره الزام	نام الزام
۴۴	**نقش های امنیتی ۲**

محصول، قادر به مرتبط نمودن کاربران با نقش های مجاز تعریف شده می باشد.

شماره الزام	نام الزام

شماره الزام	نام الزام
۴۵	**لغو مشخصه های امنیتی ۱**
محصول می تواند توانایی لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیر فعال تحت کنترل خود را به مدیر سیستم محدود نماید.	

۶.۵ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	نام الزام
۴۶	حفظ وضعیت امن در زمان شکست ۱
محصول می تواند در زمان رخداد انواع شکست های زیر، وضعیت امن را حفظ نمایند: شکست های نرم افزاری، سخت افزاری و شبکه ای **توضیح**: 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.	

شماره الزام	نام الزام
۴۷	**سازگاری داده های امنیتی بین محصول و موجودیت امن ۱**

شماره الزام	نام الزام
محصول در صورت استفاده از محصولات امن IT ، می تواند تفسیر سازگار ممیزی، شناسه کاربری و رمز عبور را در زمان اشتراک گذاری داده های امنیتی بین خود و دیگر محصولات امن IT فراهم آورد. **توضیح**: 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	

شماره الزام	نام الزام
۴۸	**انتقال داده امنیتی در داخل محصول ۱**
محصول می تواند هنگام انتقال داده ها بین بخش های مجزای خود، در برابر افشاء یا تغییر محافظت نماید.	

شماره الزام	نام الزام
۴۹	**مهرهای زمانی ۱**
محصول، می تواند قادر به ایجاد مهره های زمانی قابل اطمینان باشند.	

۷.۵ کلاس دسترسی به محصول

شماره الزام	نام الزام
۵۰	محدودیت بر روی چندین نشست همزمان ۱
محصول می تواند حداکثر تعداد نشست های همزمان متعلق به یک کاربر را محدود نماید.	

شماره الزام	نام الزام
۵۱	**محدودیت بر روی چندین نشست همزمان ۲**
محصول می تواند به صورت پیش فرض، یک نشست برای هر کاربر در نظر بگیرد.	

شماره الزام	نام الزام
۵۲	**قفل کردن و خاتمه دادن به نشست ها ۵**
محصول می تواند کلیه نشست های تعاملی راه دور (Remote) را پس از مدت زمان قابل تنظیم توسط مدیر غیرفعال بودن، خاتمه دهد.	

شماره الزام	نام الزام
۵۳	**قفل کردن و خاتمه دادن به نشست ها ۶**
محصول می تواند اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد.	

شماره الزام	نام الزام

شماره الزام	نام الزام
۵۴	**سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست براساس روز، زمان می باشد.	

۸.۵ کلاس کانالها / مسیرهای مورد اعتماد

شماره الزام	نام الزام
۵۵	**کانال امن ۱**
محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS 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 احراز هویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	

شماره الزام	نام الزام
۵۶	**کانال امن ۲**
محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	

شماره الزام	نام الزام

شماره الزام	نام الزام
۵۷	کانال امن ۳
محصول مورد ارزیابی می تواند ارتباطات را از طریق کانال امن، برای سرویس دهی به کاربران راه اندازی نماید.	

شماره الزام	نام الزام
۵۸	مسیر امن ۱
محصول، می تواند مسیر ارتباطی امنی را با استفاده از پروتکل TLS, HTTPS برای ایجاد کانال ارتباطی امن بین خود و مدیر سیستم راه دور را داشته که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آن را احراز هویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	

شماره الزام	نام الزام
۵۹	مسیر امن ۲
محصول مورد ارزیابی می تواند به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	

شماره الزام	نام الزام

شماره الزام	نام الزام
۶۰	مسیر امن ۳
محصول مورد ارزیابی می تواند استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت های راه دور مدیر سیستم الزامی کند.	

۹.۵ بروزرسانی امن

شماره الزام	نام الزام
۶۱	بروز رسانی امن ۲
محصول مورد ارزیابی می تواند این امکان را برای مدیر سیستم امنیتی فراهم کند که بروزرسانی نرم افزار و میان افزار محصول مورد ارزیابی را به صورت دستی آغاز نماید و از هیچ مکانیسم به روزرسانی دیگری پشتیبانی نکند.	

شماره الزام	نام الزام
۶۲	بروز رسانی امن ۳

شماره الزام	نام الزام
محصول مورد ارزیابی می تواند در صورت استفاده از بروزرسانی به روش خودکار، پیش از نصب بروزرسانی های نرم افزاری و میان افزاری، با استفاده از درهم ساز منتشرشده، ابزاری را برای احراز هویت میان افزار آنها در اختیار محصول مورد ارزیابی قرار دهد.	

۶ الزامات تضمین امنیت

۱.۶ بروزرسانی امن

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (ADV_FSP)	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2D)** **شرح مولفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آمادهسازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می گردند. از آنجا که مشخصات کارکردی

	مستقیماً با الزامات کارکرد امنیتی مرتبط شده اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی باشد.

مولفه های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (ADV_FSP)	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی (SFR-enforcing TSFI) پشتیبان کنندهی الزام کارکرد امنیتی (SFR-supporting TSFI) توصیف نماید
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2C)** **شرح مولفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.3C)** **شرح مولفه:** مشخصات کارکردی باید برای دسته بندی ضمنی واسط های غیر مداخله کننده ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.4C)** **شرح مولفه:** ردیابی باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (ADV_FSP)	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه های محتوایی را برآورده می نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2E)** **شرح مولفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می باشند.

۲.۶ کلاس راهنمای کاربر

۱.۲.۶ راهنمای کاربردی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (AGD_OPE)	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.1C)** **شرح مولفه:**

	سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.2C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط های در دسترس ارائه شده توسط محصول به صورت امن استفاده می گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.3C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.4C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.5C)** **شرح مولفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.6C)**

	شرح مولفه: سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.7C)** **شرح مولفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد

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

۲.۲.۶ راهنمای آماده سازی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی (AGD_PRE)	**نام عنصر: راهنمای آماده سازی ۱** **شماره مولفه: (AGD_PRE.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول را همراه با سند آماده سازی ارائه نماید.

مولفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**

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

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

۳.۶ کلاس تست

۱.۳.۶ تست مستقل

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

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

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آزمون مستقل (ATE_IND)	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مولفه های محتوایی را برآورده می نماید.

	نام عنصر: آزمون مستقل ۱ **شماره مولفه: (ATE_IND.1.2E)** **شرح مولفه:** ارزیاب باید زیرمجموعه ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می نمایند.

۴.۶ کلاس آسیب پذیری

۱.۴.۶ تحلیل آسیب پذیری

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

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

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**

آسیب پذیری (AVA_VAN)	**نام عنصر: آسیب پذیری ۱** **شماره مولفه: (AVA_VAN.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه های محتوایی را برآورده می نماید.
	نام عنصر: آسیب پذیری ۱ **شماره مولفه: (AVA_VAN.1.2E)** **شرح مولفه:** ارزیاب باید برای شناسایی آسیب پذیری های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب پذیری ۱ **شماره مولفه: (AVA_VAN.1.3E)** **شرح مولفه:** ارزیاب باید براساس آسیب پذیری های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می گیرند، مشخص نماید.

۵.۶ کلاس پشتیبانی از چرخه حیات

۱.۵.۶ قابلیت های پیکربندی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر: برچسب گذاری محصول۱** **شماره مولفه: (ALC_CMC.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر: برچسب گذاری محصول۱** **شماره مولفه: (ALC_CMC.1.1C)** **شرح مولفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت های پیکربندی (ALC_CMC)	**نام عنصر: برچسب گذاری محصول۱** **شماره مولفه: (ALC_CMC.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را برآورده می نماید.

۲.۵.۶ حوزه پیکربندی

مولفه های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی (ALC_CMC)	**نام عنصر: پوشش پیکربندی محصول۱** **شماره مولفه: (ALC_CMS.1.1D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه های اقدامات محتوایی

نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMC)	**نام عنصر: پوشش پیکربندی محصول۱** **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول۱ **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی (ALC_CMC)	**نام عنصر: پوشش پیکربندی محصول۱** **شماره مولفه: (ALC_CMS.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را برآورده می نماید.

۷ خلاصه مشخصات محصول

نسخه ۱.۰ سند هدف امنیتی سیستم بایوآرک توسط کمیته توسعه شرکت زیست داده پرداز آرکا تدوین شده است و رعایت الزامات کارکرد امنیتی زیر در آن ادعا شده است:

- شناسایی و احراز هویت

محصول مستقل از سیستم عاملی که بر روی آن اجرا می شود، قابلیت شناسایی و احراز هویت را ارائه می نماید. این شاخصه امنیتی از دسترسی کاربران غیرمجاز به سیستم جلوگیری و محافظت می نماید. همچنین این ویژگی هر کاربر را ملزم به شناسایی و احراز شدن هرگونه دسترسی به اطلاعات و کارکردهای می نماید. در صورت شکست خوردن شناسایی و احراز هویت، هدف ارزیابی هرگونه درخواستی را رد می

نماید و به صفحه Login ارجاع می دهد. علاوه بر این سرپرست سیستم می تواند احراز هویت هایی که با شکست مواجه می شوند را مدیریت نماید.
همچنین اگر تاریخ انقضا برای حساب کاربری تعریف شود، سیستم امکان غیرفعال نمودن حساب کاربری به صورت خودکار را در شرایطی که تاریخ به مقدار مشخص شده توسط سرپرست برسد را فراهم نموده 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 می باشد و می تواند 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، می تواند 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.
- 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 احراز هویت 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.
- زمانیکه یک نشست جدید برقرار می شود، اطلاعات موجود از نشست های قبلی حذف می گردد. اطلاعات پیشینه احراز هویت بروزرسانی می شود. رکورد ممیزی برای ورود موفق/ناموفق کاربر در نشست جدید ثبت می گردد.
- 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 می تواند 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 پی شفرض، 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 غیرفعال، مقادیر پیش فرض را لغو و تغییر دهد.

- محصول می تواند توانایی تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، ایجاد کاربر جدید، داده های ممیزی و داده های احراز هویت را به مدیر سیستم و توانایی تغییر پیش فرض، پرس و جو، تغییر 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 نقش های مجاز تعریف شده مرتبط نماید و امکان لغو نام کاربری مربوط به موجودیت های فعال و لغو مشخصه امنیتی یک موجودیت غیرفعال تحت کنترل خود را به مدیر سیستم محدود کند.
- 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 بخش های مجزای خود، از آنها در برابر افشاء یا تغییر محافظت نماید.
- محصول، قادر به ایجاد مهرهای زمانی قابل اطمینان می باشد.
- محصول می تواند کلیه نشست های 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 موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی و سرور احراز هویت که به طور منطقی از کانال های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. همچنین محصول می تواند اجازه داشته باشد به موجودیت های 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.