به نام خدا

الزامات امنیتی برنامه‌های کاربردی تحت شبکه

شرکت مهندسی هرمزان نیروی ایرانیان (مهنا)

سند هدف امنیتی (ST)

نرم‌افزار مدیریت حوادث برق و ثبت خاموشی (مهنا ۱۲۱)

نسخه نرم‌افزار 26

اسفند -۱۴۰۱

نسخه سند: ۳.۱

تهیه کننده: امین علی‌بلندی

فهرست

۱ معرفی محصول

نرم‌افزار مدیریت حوادث برق و ثبت خاموشی (MAHNA-121) یک نرم‌افزار کاربردی دسک‌تاپی (Desktop Application) برای ثبت حوادث است.

اصلی ترین کاربرد نرم افزار ثبت خاموشی، ثبت درخواست ها و خاموشی های مشترکین برق می‌باشد. تفکیک و پالایش به موقع این اطلاعات و هدایت آن به مسیر درست، باعث افزایش بهره‌وری در استفاده از منابع در سازمان‌های هدف می‌گردد.

این نرم افزار دارای بخش‌های مختلف زیر است:

- واحد اپراتوری، شامل زیربخش‌های: ایجاد پرونده / اعلان‌های عمومی و پیام‌های اضطراری / مرکز تماس / مشاهده وضعیت مناطق و شبکه برق / سوابق پرونده‌ها / و غیره
- واحد اتفاقات، شامل زیربخش‌های: مدیریت و پیگیری خاموشی‌ها / ارجاع و پیگیری ارجاعات بین واحدهای مربوطه / ثبت تجهیزات مصرفی / و غیره
- بخش شبکه و بارگیری‌ها، دارای زیربخش‌های: ساختار شبکه برق / بارگیری شبکه / بارگیری فشار متوسط / و غیره
- بخش آمار، جهت دریافت آمار از امور مختلف: اقدام شده، تعداد اکیپ‌های اعزام شده و ... با قابلیت فیلتر زمان و تاریخ.
- بخش گزارش‌گیری، شامل زیربخش‌های: گزارش‌های کنترلی / گزارش‌های خاموشی / گزارش عملکرد کاربران / و غیره

۱,۱ ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	نسخه نرم افزار v26
مدل و نسخه سیستم‌عامل	Windows Server 2022 Datacenter (21H2)
مدل و نسخه وب‌سرور	Not used in the OMS desktop application
مدل و نسخه پایگاه داده	SQL Server 2019
زبان برنامه‌نویسی	C#

۲,۱ معماری محصول

شرح عملکرد نرم‌افزار:

پس از ثبت رکوردها توسط اپراتورهای سامانه، کار توسط اپراتورهای مناطق مشاهده می شود که وظیفه برنامه ریزی و رسیدگی به آنها را دارند تا اگر مشترک بی برق شده با اعزام مامور و رفع مشکل، برق دار شود.

همچنین در صورت نیاز به تعمیرات یا تغییرات در شبکه برق، واحد دیسپاچینگ با برنامه ریزی با اطلاع قبلی، شبکه را بی برق میکند تا ماموران بتوانند اقدامات لازم را انجام دهند. برای اطلاع رسانی خاموشی های بابرنامه و پیگیری آن از پنل "بابرنامه" استفاده میشود.

تمامی رکوردها قابلیت جستجو و فیلتر شدن را دارند و همچنین از قابلیت‌های دیگر نرم افزار میتوان به گزارش گیری اشاره کرد که شامل گزارش حوادث، گزارش بارگیری ها، گزارش تجهیزات از قبیل پست توزیع و فیدر، گزارش عملکرد پرسنل و... می باشد.

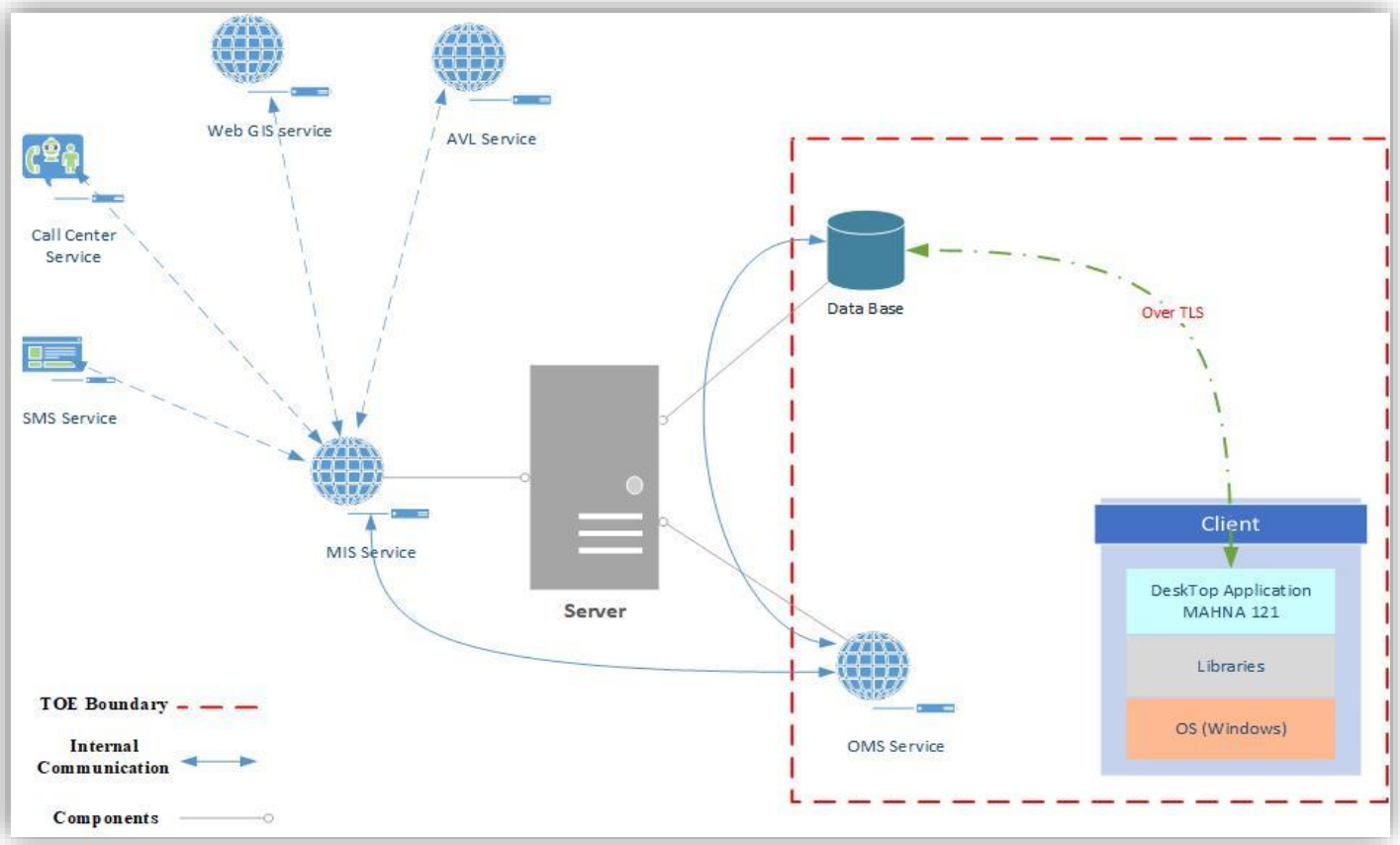
اطلاعات شبکه و بارگیری در نرم افزار ثبت شده و قابلیت بروزرسانی را دارد و امکان انجام محاسبات در بخش شبکه فشار ضعیف شبکه برق را در نرم افزار فراهم میسازد.

تنظیمات بسیار متعدد و متنوعی در نرم افزار وجود دارد که فرایندهای مربوط به بیزینس اپلیکیشن توسط مدیر سیستم پیکربندی می گردد. مدیر سیستم امکان تعریف/ویرایش و همچنین اختصاص نقش‌های مشخص شده به کاربران را دارد. دسترسی های مختلف نیز به نقشها و به کاربران داده می شود.

نام مولفه	توضیح
Desktop Application	اصلی ترین کاربرد نرم افزار ثبت خاموشی، ثبت درخواست ها و خاموشی های مشترکین برق می‌باشد. تفکیک و پالایش به موقع این اطلاعات و هدایت آن به مسیر درست، باعث افزایش بهره‌وری در استفاده از منابع در سازمان‌های هدف می‌گردد
Data Base	پایگاه داده اصلی نرم افزار می باشد.
oms service	ارسال پاره ای از اطلاعات به بخش های مختلف و همچنین دریافت و پردازش اطلاعات

: OMS Service

این سرویس وظیفه انجام عملیات محاسباتی (وصل خاموشی، محاسبه انرژی توزیع نشده و اطلاعات تکمیلی ارسالی از تبلت) و اعمال خاموشی (اطلاعاتی درباره خاموشی که از سامانه های برق من و مرکز تماس که مشترکین ثبت نموده اند به oms ارسال می‌شوند و این سرویس اطلاعات را پردازش و در دیتابیس ذخیره میکند) همچنین مدیریت خاموشی از سرویس‌ها و برنامه های گفته شده به ثبت خاموشی (برنامه ۱۲۱) می باشد. و نیز وظیفه اطلاع رسانی خاموشی به سامانه های دیگر مانند: سامانه برق من، تبلت، web gis وسرویس MIS و مرکز تماس را نیز دارد.



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

۲ الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱.۱ نمایه[1] حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر رده در نمایه‌ی حفاظتی مربوطه، یک دسته الزام بیان شده است.

۱/۲ کلاس ممیزی امنیت (Log)

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
۱	**محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[2] تولید کند (Log ثبت نماید).**			☑	
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	☑		
		تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		خواندن اطلاعات از ثبت‌نشان‌ها	☑		باز کردن بخش مدیریت سوابق بابت خواندن اطلاعات از ثبت نشان ها، لاگ ایجاد می شود.
		تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	☑		
		عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	☑		
		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	☑		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	☑		

[1] Profile
[2] Log

شماره الزام	رده ممیزی امنیت (Log)			توضیحات
	تمام کاربردهای سازوکار احراز هویت	☑		
	نتایج نهایی عملیات احراز هویت	☑		این موضوع در بخش سوابق ورود نیز قابل مشاهده است.
	تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	☑		
	شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	☑		
	تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	☑		
	تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	☑		
	تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	☑		
	همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑		
	تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑		
	استفاده از کارکردهای مدیریتی	☑		
	تغییرات در گروه کاربران	☑		
	شکست در کارکردهای امنیتی محصول	☑		در صورتی که در لاگ ممیزی، عملیات شناسایی احراز هویت و دیگر کارکردهای امنیتی نرم افزار شکستی رخ دهد، exception هایی رخ داده ولاگ آن ایجاد می شود.
	تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	☑		
	تلاش موفق یا ناموفق برای برقراری نشست.	☑		

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
		ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	☑		در صورتی که در تنظیمات نرم افزار نشست همزمان محدود شده باشد، از ایجاد نشدن نشست همزمان لاگ ممیزی ایجاد می شود.
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	☑		
		خاتمه به نشست غیرفعال توسط مدیر سیستم	☑		
		سایر موارد	☐		
۲	**محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.**			☑	
	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	تاریخ و زمان رویداد	☑		
		نوع رویداد	☑		
		هویت ایجادکننده رویداد	☑		
		نتیجه رویداد	☑		
		آدرس IP ایجادکننده رویداد	☑		
		سایر موارد	☐		
۳	**محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.**			☑	با توجه به وجود مکانیزم کنترل دسترسی ، از دسترسی غیرمجاز به لاگ ها جلوگیری می شود.
۴	**ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			☑	
	مواردی که در ثبت‌نشان‌ها وجود	نبود داده نامفهوم در رکوردها	☑		
		نبود بخش‌های نامرتبط	☑		

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
	دارند، مشخص شوند.	وجود داده معتبر و مناسب در هر بخش	☑		
۵	**محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			☑	
	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	هویت موجودیت فعال	☑		
		نوع حساب کاربری	☑		
		تاریخ/زمان	☑		
		روش اتصال کاربر	☐		با توجه به اینکه تمامی اتصال ها از طریق باز شدن نرم افزار تحت ویندوز صورت میگیرد، روش اتصال همیشه یکسان است.
		نوع رخداد	☑		
		مکان رویداد	☑		
		سایر موارد	☐		
۶	**محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.**			☑	
	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	☑		
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☑		
		فقط خواندنی کردن ثبت‌نشان‌ها در محصول	☑		
		سایر موارد	☐		

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
۷	**محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**			☑	
	روش‌های اطلاع‌رسانی مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐		
		ارسال پیام	☑		با استفاده از یک سرویس ارسال پیامک، زمانی که حجم لاگ ها به اندازه آستانه تعیین شده در تنظیمات برسد، یک پیام اخطار ارسال می شود.
		از طریق واسط کاربر مجاز	☐		
		سایر موارد	☐		
۸	**محصول باید توانایی تولید ثبت‌نشان (ثبت Log) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.**			☑	
	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن ثبت‌نشان‌ها	☐		
		ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☐		
		بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده	☑		
		سایر موارد	☐		

۲,۲ کلاس رمزنگاری

شماره الزام	رده رمزنگاری				توضیحات
۱	**محصول باید قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			☑	
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38A)	☐		
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	☑		استفاده از مد GCM با طول کلید های ۱۲۸ و ۲۵۶
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در ISO10116)	☐		
۲	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**			☑	
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ بیت	☐		
		الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت	☑		در ارتباطات TLS
		الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت	☑		در ارتباطات TLS

شماره الزام	رده رمزنگاری				توضیحات
	نمـایـیـد. (وجود یـک مورد لازم و کافی است.)	الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت	☑		از الگوریتم SHA-512 برای درهم‌سازی در فرآیند بروزرسانی نرم افزار استفاده شده است.
۳	**در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)**			☑	
	روش نـابـودی کلیـد مشـخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☑		
		سایر موارد	☐		
۴	**در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☑	
	الگوریتم و انـدازه کلیـدهـای مورد استفاده را انتخاب نمـایـیـد. (وجود	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)	☑		الگوریتم RSA با طول کلید ۲۰۴۸

شماره الزام	رده رمزنگاری				توضیحات
	یـک مورد لازم و کافی است)	الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۶.۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☑		

۳/۲ کلاس شناسایی و احراز هویت

شماره الزام	رده شناسایی و احراز هویت				توضیحات
۱	**محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.**			☑	
	مقدار یا یازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	یک عدد مثبت ثابت	☐		
		یک عدد مثبت قابل تنظیم توسط مدیر	☑		
۲	**محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.**			☑	
	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.) لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	☑		
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	☐		

شماره الزام	رده شناسایی و احراز هویت				توضیحات
	می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)	☑		پس از رسیدن تعداد تلاش های ناموفق احراز هویت به مقدار تعیین شده در "آستانه شکست احراز هویت"، CAPTCHA نمایان می شود.
		سایر موارد	☐		
۳	**محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.**			☑	
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	☑		
		روش احراز هویت مورد استفاده	☑		
		داده احراز هویت	☑		
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	☑		
		نقش کاربر	☑		
		سایر موارد	☐		
۴	**محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.**			☑	
	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	استفاده از حروف کوچک	☑		
		استفاده از حروف بزرگ	☑		
		استفاده از اعداد	☑		

شماره الزام	رده شناسایی و احراز هویت				توضیحات
		استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...)	☑		
		حداقل طول ۸ یا بیشتر (قابل تنظیم)	☑		
		سایر موارد	☐		
۵	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**			☑	
	اقدامات عمومی که کاربر می‌تولند قبل از احراز هویت انجام دهد، انتخاب شود.	مشاهده راهنمای نحوه ورود به سیستم	☐		
		بازیابی گذرواژه	☐		
		هیچ اقدامی	☑		
		سایر موارد	☐		
۶	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).**			☑	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و گذرواژه	☑		
		امضای دیجیتال	☐		
		سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	☑		در نرم‌افزار از سرویس **اکتیو دایرکتوری** به عنوان سامانه های احراز هویت مرکزی پشتیبانی می شود.
		OTP یا توکن	☐		
		احراز هویت دو فاکتوری	☑		
		سایر موارد	☐		

شماره الزام	رده شناسایی و احراز هویت			توضیحات
۷	**محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.**		☑	
	ویژگی‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	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)	☑	پیشینه احراز هویت در بخش سوابق ورود نرم افزار، قابل مشاهده هستند.
		سایر موارد	☐	
۸	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**		☑	

شماره الزام	رده شناسایی و احراز هویت				توضیحات
	در صورتی که محصول قوانین بیشـــــــتری هنگام برقراری نشســـــــت اعمال می‌نماید، ایــن قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشست‌های قبلی هنگام برقراری یک نشست جدید (به جز مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود.)	☑		
		بروزرسانی اطلاعات پیشینه احراز هویت	☑		در بخش سوابق ورود، نسبت به هر نوع نشست موفق و یا ناموفق، اطلاعات پیشینه احراز هویت ثبت شده و قابل نمایش است.
		سایر موارد	☐		
۹	**محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			☑	
	قوانینی کـه در صـــورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑		
		سایر موارد	☐		

۴/۲ کلاس حفاظت از داده کاربری

شماره الزام	رده حفاظت از داده‌ی کاربری				توضیحات
۱	**محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر عادی	☑		
		سایر موارد	☐		
	موجودیت‌های غیرفعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	سوابق، مستندات و فراداده	☑		
		داده متعلق به کاربران	☑		
		داده احراز هویت	☑		
		سایر موارد	☐		
	عملیاتی که خط‌مشی‌های کنترل دسترسی در رابطه با آنها اعمال می‌شوند، مشخص گردد.	ایجاد موجودیت غیرفعال جدید	☑		
		حذف موجودیت غیرفعال	☑		
		تغییر دسترسی‌ها به موجودیت غیرفعال	☑		
		عملیات بر روی فراداده وابسته به موجودیت غیرفعال	☑		
		سایر موارد	☐		

شماره الزام	رده حفاظت از داده‌ی کاربری				توضیحات
۲	**محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	ویژگی‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	☑		
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	☑		
		سایر موارد	☐		
۳	**محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.)**			☑	
۴	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			☑	
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	☑		
		سایر موارد	☐		

شماره الزام	رده حفاظت از داده‌ی کاربری			توضیحات
۵	**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.**		☑	اطلاعات قبلی یک منبع در نرم افزار، آزادسازی می‌شود و کاربر بعدی به اطلاعات قبلی دسترسی ندارد. همچنین طبق مکانیزم‌هایی داده های موجود در Memory پس از بستن نرم افزار، Deallocate می شوند.
۶	**محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**		☑	
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	نوع داده	☑	در بخش تنظیمات، تنظیمات دارایی، قسمت تعیین فایل های ورودی، امکان انتخاب فرمت های: Doc, Docx, Xls, jpg, Xlsx, Gif, jpeg, PDF, png وجود دارد.
		حجم و اندازه	☑	امکان تعیین حجم و اندازه ی فایل های ورودی در بخش تنظیمات امنیتی نرم‌افزار، وجود دارد
		فرمت	☑	در بخش تنظیمات، تنظیمات دارایی، قسمت تعیین فایل های ورودی، امکان انتخاب فرمت های: Doc, Docx, Xls, jpg, Xlsx, Gif, jpeg, PDF, png وجود دارد.
		تعداد دفعات Import	☐	
		سایر موارد	☐	
۷	**محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.**		☑	برای انتقال داده از نرم‌افزار به پایگاه داده از پروتکل امن TLS (TDS Over TLS) استفاده شده است.

شماره الزام	رده حفاظت از داده‌ی کاربری				توضیحات
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	نوع داده	☑		در نرم‌افزار امکان انتقال داده به بیرون از محصول با به صورت pdf و اکسل وجود دارد.
		حجم و اندازه	☐		
		فرمت	☑		در نرم‌افزار امکان انتقال داده به بیرون از محصول با با فرمت pdf و xls وجود دارد.
		سایر موارد	☐		
۹	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**			☑	
	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☑		با استفاده از مکانیزم احراز هویت مجدد در زمانی که کاربر مجاز قصد خروج داده از محصول را داشته باشد، عملیات Export محدود به کاربر مجاز با وارد کردن کلمه عبور می شود.
		سایر موارد	☐		
۱۰	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.**			☑	
		مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	☑		

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

۵/۲ کلاس مدیریت امنیت

شماره الزام	رده مدیریت امنیت			توضیحات
۱	**محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.**		☑	
	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	تعیین و تغییر رفتار	☑	
		غیرفعال نمودن	☐	
		فعال نمودن	☐	
		سایر موارد	☐	
۲	**محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**		☑	
	عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	پرس‌وجو	☑	
		تغییر	☑	
		حذف	☑	
		تغییر پیش‌فرض	☑	
		سایر موارد	☐	
۳	**محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**		☑	

شماره الزام	رده مدیریت امنیت				توضیحات
	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.	تغییر پیش‌فرض	☑		
		حذف نمودن	☑		
		پرس‌وجو	☑		
		مقداردهی	☑		
		ایجاد	☑		
		مشاهده	☑		
		سایر موارد	☐		
۴	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			☑	
	در صورتی که هرکدام از موارد مطرح‌شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	☑		در نرم افزار بر اساس ساختار اختصاص نقش به هر کاربر، قابلیت اختصاص نقش قابلیت خواندن و مشاهده لاگ ها (توسط ادمین و کاربر مجاز در اعمال تنظیمات) وجود دارد.
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	☑		فقط کاربر مجاز که امکان دسترسی به بخش لاگ ها به وی داده شده است، قادر به مشاهده خواهد بود.
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها	☑		
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	☑		

شماره الزام	رده مدیریت امنیت				توضیحات
		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 تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	☑		
		۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	☑		
		مدیریت معیارها برای تنظیم گذرواژه‌ها	☑		
		۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.	☑		
		۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	☑		
		مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از	☑		

شماره الزام	رده مدیریت امنیت				توضیحات
		این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.			
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	☑		
		مدیریت نقش‌ها در محصول	☑		
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	☑		
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑		
		۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. ۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	☑		
۵	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**			☑	
		مدیر سیستم	☑		
		کاربر پیشرفته	☑		

شماره الزام	رده مدیریت امنیت				توضیحات
	نقش‌هایی که در محصول پشتیبانی می‌شوند، مشخص گردد.	کاربر عادی	☑		
		سایر موارد	☐		
۶	**محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.**			☑	

۶/۲ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
۱	**محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.**			☑	
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	خرابی‌های نرم‌افزاری	☑		
		خرابی‌های سخت‌افزاری	☑		
۲	**محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.**			☑	ارتباط بین نرم‌افزار و پایگاه داده، با استفاده از پروتکل TLS نسخه ۱.۲رمزنگاری شده و از افشای اطلاعات جلوگیری شده است.
۳	**در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.**			☑	
	داده امنیتی قابل اشتراک‌گذاری که در	داده‌های احراز هویت	☑		
		کلید	☐		
		امضای دیجیتال	☐		

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
	محصول پشتیبانی می‌شوند، مشخص گردد.	ثبت‌نشان‌ها (داده‌های ممیزی)	☐		
		سایر موارد	☐		
۴	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[۳] معتبر را تولید یا از آن‌ها استفاده نماید.**			☑	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐		
		تنظیم مهرهای زمانی از طریق اینترنت	☐		
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	☑		
		سایر موارد	☐		
۵	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**			☑	
	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروزرسانی دستی	☑		
		جستجوی خودکار بروزرسانی‌ها	☑		هر بار که نرم افزار اجرا می‌شود، طبق یک تابع، عملیات بررسی نسخه فعلی با آخرین نسخه منتشر شده در update server صورت میگیرد.
		بروزرسانی‌های خودکار	☑		
		بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	☐		

[3] Time stamp

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
۶	**در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**			☑	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضای دیجیتال	☐		
		درهم‌ساز منتشرشده	☑		برای افزایش امنیت سازوکار بروزرسانی نرم افزار، مدیر مجاز مقدار درهم سازی تولید شده توسط یک نرم افزار را داخل جدول تنظیمات در پایگاه داده قرار میدهد. برنامه زمانی که یک بروز رسانی برای آن در دسترس باشد ابتدا فایل بروزرسانی را گرفته و با استفاده از ساز و کاری قبل از فایل دانلود شده درهم سازی تولیده میکند، اگر مقدار درهم سازی تولید شده با مقدار درج شده در پایگاه داده یکسان باشد برنامه unzip میشود و نرم افزار بروز میگردد ولی اگر مقادیر درهم سازی شده یکسان نباشند نرم افزار اجازه بروزرسانی نمیدهد و فایل دانلود شده پاک میشود.

۷/۲ کلاس تخصیص منابع

شماره الزام	رده تخصیص منابع		توضیحات
۱	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	☑	در نرم افزار، زمانی که شکست و خرابی رخ داده و ارتباط با پایگاه داده و دیگر سرویس‌های مهم برقرار نشود، از ادامه کار جلوگیری میشود. با مدیریت خطای مناسب از پایداری عملکرد محصول در حفظ شرایط مناسب و جلوگیری از اختلال، اطمینان حاصل می شود

۸/۲ کلاس دسترسی به محصول

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

شماره الزام	رده دسترسی به محصول				توضیحات
۶	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**			☑	در بخش سوابق ورود، با فیلتر تاریخ و ساعت، همیشه امکان دسترسی به سوابق تلاش های موفق و ناموفق وجود دارد و این موضوع هیچگاه از دسترس کاربر خارج نخواهد شد.
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**			☑	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	مکان	☑		
		شماره پورت	☐		
		روز	☐		
		زمان	☐		
		سایر موارد	☐		

۹/۲ کلاس کانال‌ها / مسیرهای مورد اعتماد

شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد				توضیحات
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 دهد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد.** در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۲-۳- و ۴-۳- که در بخش ۳- **Error! Reference source not found.** بیان گردیده است، الزامی است.		☑		
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	☑		
		TLS	☑		ارتباط بین نرم‌افزار با سرور پایگاه داده، با استفاده از پروتکل TLS نسخه 1.2 رمز می‌شود.
		SSH	☐		
۲	**محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.**		☑		
۳	**محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.**		☑		

۳ الزامات امنیتی مبتنی بر انتخاب

این بخش به بیان الزاماتی می‌پردازد که رعایت آنها وابسته به برخی از الزاماتی است که در بخش‌های پیشین بیان شده است.

۱،۳ پروتکل HTTPS

شماره الزام	پروتکل HTTPS				توضیحات
۱	**محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.**			☑	
۲	**محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.**			☑	
۳	**در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید.** اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۵.۳ انجام می‌شود که در این صورت الزامات بخش ۵.۳ الزامی است.			☑	
	محصول تنها از موارد بیان‌شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	☑		
		برای برقراری اتصال درخواست مجوز کند.	☐		

۲/۳ کلاس پروتکل TLS Client

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

شماره الزام	پروتکل TLS Client			توضیحات
			0xC02C مطابق با RFC 5289	
		☑	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289	
		☐	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288	
		☐	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288	
		☐	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288	
		☐	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289	
		☐	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289	
		☐	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289	
		☐	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1	

شماره الزام	پروتکل TLS Client				توضیحات
			مطابق با RFC 5288		
			TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288	☐	
۲	**محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.**			☑	
۳	**محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.		ارتباط را برقرار نکند	☑	
			برای برقراری ارتباط درخواست مجوز کند	☐	
			سایر موارد	☐	
۴	**محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.**			☐	
	در صورتی که محصول از خم‌های بیضوی استفاده می‌نماید،		Supported Elliptic Curves Extension را ارائه نکند.	☐	
			Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.	☑	با استفاده از secp384r1 طبق لیست جدید خم های امن و مجاز

شماره الزام	پروتکل TLS Client				توضیحات
	نوع خم باید مشخص گردد.				

۳/۳ کلاس پروتکل TLS Server

شماره الزام	پروتکل TLS Server				توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446	☐		
		TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446	☐		
		TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288	☑		
		TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288	☑		
		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289	☑		
		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289	☑		
		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289	☐		

شماره الزام	پروتکل TLS Server				توضیحات
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289		
		☐	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288		
		☐	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288		
		☐	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288		
		☐	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289		
		☐	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289		
		☐	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289		
		☐	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288		
		☐	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0		

شماره الزام	پروتکل TLS Server				توضیحات
		مطابق با RFC 5288			
۲	**محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1دارند را رد نماید.**		☑		
۳	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**		☑		
	طولی کلید یا نوع خم مورد استفاده باید مشخص گردد.	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	☐		
		پارامترهای ECDH(E) با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر	☑		از خم بیضوی secp384r1 استفاده شده است.
		پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت	☑		از اندازه کلید ۲۰۴۸ بیت استفاده شده است

٤,٣ پروتکل TLS مشترک کلاینت و سرور

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

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

۵,۳ اعتبارسنجی گواهی‌نامه

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
۱	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			☑	
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		
		محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	☑		
	روش‌های تأیید وضعیت فسخ گواهی‌نامه	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص‌شده در RFC 696	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶.۳	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵	☐		
		هیچ روش فسخ دیگری	☐		
		گواهی‌نامه‌های مورد استفاده برای تأیید بروزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing»	☐		

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
	قوانین تأیید بخش extendedKeyUsage	(id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.			
		گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف « Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.	☑		
		گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند.	☐		
		گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در بخش extendedKeyUsage خود داشته باشند.	☐		
۲	**محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.**			☑	
۳	**محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند.**			☑	
	در صورت پشتیبانی از کارکردهای دیگر،	HTTPS	☑		
		TLS	☑		
		SSH	☐		
		امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	☐		

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
	در «ســـایر موارد» بیان گردد.	امضای کد برای تأیید یکپارچگی	☐		
		سایر موارد	☐		

۶/۳ پروتکل SSH

شماره الزام	پروتکل SSH				توضیحات
۱	**محصول باید پروتکل SSH را مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.**	☐			کاربرد ندارد
۲	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.**	☐			
	احراز هویت مبتنی بر کلید عمومی	☐			
	احراز هویت مبتنی بر گذرواژه	☐			
۳	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.**	☐			
۴	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.**	☐			
	AES128-CBC	☐			
	AES192-CBC	☐			
	AES256-CBC	☐			
	AES128-CTR	☐			
	AES192-CTR	☐			
	AES256-CTR	☐			
	AEAD_AES_128_GCM	☐			
	AEAD_AES_256_GCM	☐			

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

شماره الزام	پروتکل SSH			توضیحات
۷	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.**	☐		
	curve25519-sha256	☐		
	curve448-sha512	☐		
	diffie-hellman-group-exchange-sha256	☐		
	diffie-hellman-group18-sha512	☐		
	diffie-hellman-group17-sha512	☐		
	diffie-hellman-group16-sha512	☐		
	diffie-hellman-group15-sha512	☐		
	ecdh-sha2-nistp521	☐		
	ecdh-sha2-nistp384	☐		
	ecdh-sha2-nistp256	☐		
	rsa2048-sha256	☐		
	diffie-hellman-group-exchange-sha1	☐		
	diffie-hellman-group14-sha256	☐		
۸	**محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (طول نشست بیشتر از یک ساعت و حجم داده مبادله شده بیشتر از ۱ گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.**	☐		
۹	**محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن (تشریح‌شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.**	☐		