به نام خدا

سند الزامات امنیتی
برنامه‌های کاربردی تحت شبکه

محصول: سامانه مرکزی مدیریت محتوا

شرکت: کارآمدان ماندگار سیستم

نسخه سند: ۲

نسخه محصول منطبق با این سند: ۱.۱.۳

تاریخ تنظیم سند: خرداد ماه ۱۴۰۲

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد موردنیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. سند هدف امنیتی بر اساس اسنادی که پروفایل‌های حفاظتی نامیده می‌شوند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یک محصول افتایی می‌بایست رعایت گردد. از آنجا که متن این پروفایل‌ها پیچیده بوده و لذا تهیه سند هدف امنیتی کاری زمان‌بر برای تولیدکننده است، ساده‌سازی الزامات امنیتی موجود در پروفایل‌های حفاظتی به نحوی که برای تولیدکننده مشخص شود که چه مواردی امنیتی باید در یک محصول خاص رعایت شود، بسیار مفید خواهد بود.

سند پیش‌رو حاوی الزامات امنیتی «پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه» که سعی شده است تا حد ممکن ساده و قابل‌فهم گردد، است. این سند دو هدف را دنبال می‌کند. اول آنکه موارد امنیتی را که باید در محصول رعایت شود (تا منجر به دریافت گواهی امنیتی گردد) برای تولیدکننده مشخص نماید و ثانیاً، تدوین سند هدف امنیتی را که کاری زمان‌بر است را تولیدکننده سریع و آسان نماید.

فهرست

۱ مقدمه

سند هدف امنیتی، یکی از اسنادی است که تولیدکننده می‌بایست قبل از شروع آزمون ارزیابی امنیتی تدوین نماید. بر اساس استاندارد معیار مشترک (CC) این سند مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تهیه می‌شود. متن پروفایل‌های حفاظتی اغلب ثقیل بوده و تسلط بر مفاهیم آن‌ها زمان‌بر است. در این راستا مرکز افتا با همکاری آزمایشگاه‌های ارزیابی امنیتی، به منظور چابک‌سازی فرآیند ارزیابی امنیتی، «سند الزامات امنیتی» را جایگزین پروفایل‌های حفاظتی نموده است. هدف از سند الزامات امنیتی، ساده-سازی مفاهیم الزامات مطرح شده در پروفایل‌های حفاظتی و نیز کمک به تولیدکننده در جهت سرعت بخشیدن به تدوین سند هدف امنیتی است.

این سند مجموعه‌ای از الزامات امنیتی برای برنامه‌های کاربردی تحت شبکه را مطرح می‌کند. هر محصولی که ادعای انطباق با «سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه» را داشته باشد، می‌بایست الزامات مطرح شده در آن را پیاده‌سازی نماید.

۲ الزامات امنیتی

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

۱/۲ ممیزی امنیت (لاگ)

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

شماره الزام	کلاس ممیزی (لاگ)				توضیحات
۱	**محصول باید برای موارد مشخص شده که در ذیل آمده است، رکورد ممیزی تولید کند (لاگ ثبت نماید).**			■	
	رویدادهایی که برای آن‌ها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	□		کاربر ارشد (admin) با ورود به پنل کاربری، می‌تواند با استفاده از زیر منوی log در منوی Reports به لاگ‌های ثبت شده در سامانه دسترسی پیدا کند. همچنین امکان استفاده از فیلدهای تاریخ، نوع، صفحه، تابع، کاربر و نمایشگر جهت جستجوی دقیقتر و مرتب‌سازی لاگ‌ها وجود دارد. لاگ جداگانه برای شروع و پایان توابع وجود ندارد. تنها فراخوانی هر تابع به همراه اطلاعات مورد نیاز در خصوص عمل انجام شده در یک رکورد لاگ ثبت می‌شود. تغییرات در پیکربندی لاگ شامل تعیین حد آستانه نگه‌داری لاگ در سرور براساس تعداد روز، در بخش مدیریت (Management) > تنظیمات
		تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای لاگ	□		
		خواندن اطلاعات از رکوردهای لاگ	□		
		تمامی تغییرات در پیکربندی لاگ	■		
		عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه	□		
		عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگ‌ها	□		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی.	■		
		تمام کاربردهای سازوکار احراز هویت	■		
		نتایج نهایی عملیات احراز هویت	■		
		تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول	■		
		شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال)	■		

		تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی	■		(Settings) در تب نگه‌داری (Maintenance) تنها توسط کاربر ارشد (admin) قابل تنظیم است و لاگ ویرایش این تنظیمات نیز ذخیره می‌شود.
		تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	■		
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه مشخصه‌های امنیتی)	■		
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	■		
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	■		
		استفاده از کارکردهای مدیریتی	■		
		تغییرات در گروه کاربران	■		
		شکست در کارکردهای امنیتی محصول	■		
		تمامی قابلیت‌هایی از محصول که به دلیل شکست، نمی-توانند عملیات موردنظر را انجام دهند.	■		
		تلاش موفق یا ناموفق برای برقراری نشست	■		
		عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل)	■		
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	■		
		خاتمه به نشست غیرفعال توسط مدیر سیستم	■		
		سایر موارد	□		
۲	**محصول باید برای هر رکورد ممیزی تولید شده، مشخصاتی که در ذیل آمده است را ثبت نماید.**			■	سایر موارد عبارتند از اطلاعات مرورگر و نسخه سیستم عامل کاربر، صفحه وقوع و تابع رویداد
	مشخصاتی کـه در	تاریخ و زمان رویداد	■		

	رکوردهای ممیزی وجـــــــود دارد مشخص شود.	نوع رویداد	■		
		هویت ایجادکننده رویداد	■		
		نتیجه رویداد	■		
		آدرس IP ایجادکننده رویداد	■		
		سایر موارد	■		
۳	**محصول باید رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.**			■	فقط کاربر ارشد (admin) اجازه دسترسی به بخش لاگ را دارد و امکان ایجاد دسترسی برای کاربران دیگر وجود ندارد.
۴	**رکوردهای ممیزی که محصول تولید می‌نماید باید برای کاربر ساده و قابل‌فهم باشند.**			■	
	موارد‌ی کـــه در رکوردهای ممیزی وجـــود دارنـــد، مشخص شوند.	عدم وجود داده نامفهوم در رکوردها	■		
		عدم وجود فیلدهای نامرتبط	■		
		وجود داده معتبر و مناسب در هر فیلد	■		
۵	**محصول باید امکان انتخاب و مرتب‌سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			■	کاربر ارشد در منوی گزارش‌ها (Reports) > گزارش (log) می‌تواند با استفاده از دکمه Filter به جستجو و مرتب‌سازی لاگ‌ها بپردازد. در این فیلتر، فیلدهای نوع (ممیزی، خطا)، تاریخ (از تاریخ و تا تاریخ)، صفحه، تابع، کاربر و نمایشگر وجود دارد.
	موارد‌ی کـــه بـــر اســـاس آن‌هـــا مرتب‌سازی وجـود دارد، مشـــخص	هویت موجودیت فعال	■		
		نوع حساب کاربری	□		
		تاریخ/زمان	■		
		روش اتصال کاربر	□		
		نوع رخداد	■		

	شود.	مکان رویداد	☐		
		سایر موارد	■		
۶	**محصول باید هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی را تشخیص دهد و در صورت امکان جلوگیری نماید.**			■	کاربران در پنل مدیریتی امکان ایجاد تغییر در رکوردهای لاگ را ندارند.
	روش‌های تشخیص مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از هش برای تشخیص تغییرات	☐		
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☐		
		فقط خواندنی کردن ممیزی‌ها در محصول	■		
		سایر موارد	☐		
۷	**محصول باید وقتی که حجم داده‌های ممیزی، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**			☐	تعیین حد آستانه نگه‌داری لاگ در سرور براساس تعداد روز، در بخش مدیریت (Management) > تنظیمات (Settings) در تب نگه‌داری (Maintenance) تنها توسط کاربر ارشد (admin) قابل تنظیم است و لاگ ویرایش این تنظیمات نیز ذخیره می‌شود. همچنین در صورت برزو خطا در ثبت لاگ به هر دلیل مانند پر شدن فضای حافظه، عدم سرویس‌دهی پایگاه داده نصب شده بر روی سرور و ...، لاگ مستقیما در syslog سرور ذخیره می‌شود. در صورت رسیدن به حد آستانه، از آنجایی که این حد تعداد روز نگه داری لاگ است و توسط تنها
	روش‌های اطلاع‌رسانی مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐		
		ارسال پیام	☐		
		از طریق واسط کاربر مجاز	■		
		سایر موارد	☐		

					کاربر مجاز تعیین این تنظیم یعنی کاربر ارشد تعیین می‌شود. اعلانی انجام نمی‌شود. اما در صورت ثبت لاگ به هر دلیل قبل از رسیدن به حد آستانه در syslog، این مورد در قالب هشدار در پنل کاربری به کاربر ارشد اعلان می‌شود.
۸	**محصول باید توانایی ممیزی (ثبت لاگ) هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و برای این کار از رویکردهای بیان شده استفاده نماید.**			☐	در صورت برزو خطا در ثبت لاگ به هر دلیل مانند پر شدن فضای حافظه، عدم سرویس‌دهی پایگاه داده نصب شده بر روی سرور و ...، لاگ مستقیما در syslog سرور ذخیره می‌شود. همچنین این مورد در قالب هشدار در پنل کاربری به کاربر ارشد اعلان می‌شود.
	رویکردهای مورد استفاده در محصول، مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن رویدادهای ممیزی	☐		
		ذخیره‌سازی محدود رویدادهای ممیزی، (آن‌هایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☐		
		بازنویسی روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده	☐		
		سایر موارد	■		

۲/۲ رمزنگاری

در این کلاس، توانایی محصول در پیاده‌سازی یا به‌کارگیری ماژول‌های رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده از رمزنگاری استفاده می‌گردد و این رمزنگاری‌ها می‌تواند به صورت متقارن و نامتقارن صورت گیرد. در رمزنگاری متقارن از یک کلید مشترک برای رمزگذاری و رمزگشایی، استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یک زوج کلید (کلید عمومی و کلید خصوصی) صورت می‌گیرد. الگوریتم‌ها می‌توانند با طول کلیدهای مختلف و به روش‌های

مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این کلاس، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در کلاس رمزنگاری همچنین از الگوریتم‌های درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	کلاس رمزنگاری				توضیحات
۱	**محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			☐	این سامانه تحت وب است و بر روی سرور استاندارد راه‌اندازی می‌شود.
	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 (تعریف شده در NIST SP 800- 38A)	☐		
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800- 38D)	☐		
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در ISO10116)	☐		
۲	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی‌شده (هش) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**			☐	این سامانه تحت وب است و از تابع SHA1 با طول ۱۶۰ بیت استفاده می‌کند.

	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	■		
		الگوریتم SHA-256 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
		الگوریتم SHA-384 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
		الگوریتم SHA-512 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
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 نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☐		
		سایر موارد	☐		
۴	**در صورتی که امضاء دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضاء رمزنگاری (تولید و تائید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☐	
	الگوریتم و اندازه	الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر	☐		

	کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	(بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳)			
		الگوریتم‌های امضاء 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 منحنی‌های P-256 یا P-384 یا P-521)	☐		

۳٫۲ شناسایی و احراز هویت

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

شماره الزام	کلاس شناسایی و احراز هویت		توضیحات
۱	**محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت شدن صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.**	■	تعداد تلاش مجاز به صورت پیش فرض ۳ تلاش است. این مقادیر در بخش مدیریت (Management) > تنظیمات (Settings) در تب اجازه دسترسی

	مقدار یا بازه‌ی مورد استفاده در هر مورد باید مشخص گردد. (وجود یک مورد لازم و کافی است.)	یک عدد مثبت ثابت	☐		(Permissions) تنها توسط کاربر ارشد قابل تنظیم است.
		یک عدد مثبت قابل تنظیم توسط مدیر	■		
		یک بازه‌ی قابل قبولی از مقادیر	☐		
۲	**محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.**			■	تعداد تلاش مجاز به صورت پیش فرض ۳ است و در صورت وقوع، کاربر به صورت پیش فرض برای ۵ دقیقه آتی امکان تلاش برای ورود را ندارد و در این خصوص پیام مناسب را در فرم ورود مشاهده خواهد کرد. این مقادیر در بخش مدیریت (Management) > تنظیمات (Settings) در تب اجازه دسترسی (Permissions) تنها توسط کاربر ارشد قابل تنظیم است. البته غیرفعال کردن کاربر در رابطه با کاربر ارشد اتفاق نخواهد افتاد. در خصوص کاربر ارشد از سازوکار CAPTCHA استفاده می‌شود.
	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال	غیرفعال کردن حساب کاربری (فعال کردن به‌صورت دستی توسط مدیر صورت می‌گیرد)	☐		
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به‌صورت خودکار صورت می‌گیرد)	■		
		استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)	■		
		سایر موارد	☐		

	کـــــردن حســـــاب کـــاربری در تمـــامی کاربردهـــــا مفیـــــد نیست.				
۳	**محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید.**			■	در این سامانه فقط کاربر ارشد (admin) و کاربرانی اجازه دسترسی به بخش مدیریت کاربران در منو مدیریت (Management) > کاربران (Users) را دارند، می‌توانند به تعریف و مدیریت کاربر در زیرمجموعه خود بپردازند. در تعریف کاربر نام کاربری به عنوان شناسه کاربر و کلمه عبور باید مشخص شود. هر کابر بعد از اولین ورود موظف به تغییر کلمه عبور خود است. البته مدیر هر کاربر می‌تواند به ویرایش نام کاربری و کلمه عبور وی بپردازد و وی مجددا بعد از ورود با کلمه عبور جدیدی که مدیر مربوطه تعریف کرده، موظف به تغییر کلمه عبور خود است. هر کاربر علاوه بر امکان ویرایش نام کاربری و کلمه عبور خود و کاربران زیرمجموعه خود، می‌تواند به غیرفعال کردن یا در اصطلاح این سامانه "بازنشسته" کردن کابران زیر مجموعه خود بپردازد. در این سامانه تنها نقش از پیش‌تعریف شده، کاربر
	مشخصه‌های امنیتی موردنیـــاز کـــه بایـــد بـــرای هـــر کـــاربر نگهداری شوند.	شناسه کاربر	■		
		روش احراز هویت مورد استفاده	□		
		داده احراز هویت	■		
		وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)	■		
		نقش کاربر	□		
		سایر موارد	□		

					ارشد (admin) است. این کاربر و دیگر کاربرانی که امکان تعریف کاربر در زیرمجموعه خود دارند می‌توانند در بخش مدیریت کاربران با استفاده از دو قسمت "امنیت صفحه" (Page Security) و "امنیت گزینه‌ها" (Menu Security) به تنفیظ اختیارات و ایجاد دسترسی به بخش‌ها و موجودیت‌های سامانه برای کاربران زیرمجموعه خود بپردازند.
۴	**محصول باید قابلیت مدیریت کلمه‌عبور را فراهم آورد.**			■	پیچیدگی کلمه عبور توسط کابر ارشد (admin) و با استفاده از Regular Expression در بخش مدیریت (Management) > تنظیمات (Settings) در تب اجازه دسترسی (Permissions) قابل تنظیم است. به این ترتیب همه موارد ذکر شده قابل اعمال استو شایان ذکر است به صورت پیش‌فرض، این موارد به علاوه جلوگیری تکرار یک حرف بیش از دوبار به صورت متوالی، در نظر گرفته شده است.
	موارد نیاز که باید در تعریف کلمه‌عبور استفاده شوند.	استفاده از حروف کوچک	■		
		استفاده از حروف بزرگ	■		
		استفاده از اعداد	■		
		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 می‌تواند قبل از احراز هویت انجام	مشاهده راهنمای نحوه ورود به سیستم	□		
		بازیابی کلمه‌عبور	□		
		هیچ اقدامی	■		

	دهد، انتخاب شود.	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).**			■	امکان تنظیم نحوه احراز هویت کاربران با استفاده از Active Directory (به غیر از کاربر ارشد)، توسط کاربر ارشد در بخش مدیریت (Management) > تنظیمات (Settings) در تب LDAP وجود دارد. برای استفاده از این امکان باید کاربران با استفاده از نام کاربری موجود در Active Directory در سامانه تعریف شوند. در این حالت کلمه عبور تعریف شده در سامانه بلااستفاده بوده و فقط برای احراز هویت از ارتباط با Active Directory استفاده خواهد شد.
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و کلمه‌عبور	■		
		امضاء دیجیتال	☐		
		Active directory	■		
		OTP یا توکن	☐		
		احراز هویت دو فاکتوری	☐		
		سایر موارد	☐		
۷	**محصول باید برای هر کاربر فعال، مشخصه‌های امنیتی نگهداری نماید.**			■	علاوه بر موارد ذکر شده، آخرین صفحه سامانه که مورد استفاده کاربر قرار گرفته و زمان دقیق آن و همچنین آدرس IP کاربر نیز نگه‌داری می‌شود. اطلاعات هر نشست فعال در بخش گزارش‌ها (Reports) > نشست‌ها (Sessions) توسط کاربر ارشد قابل مشاهده است.
	مشخصه‌هایی 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	شناسه کاربر	■		
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه	☐		
		جزئیات واسط کلاینت	■		
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☐		
		سایر موارد	■		

	موارد» بیان می‌شوند).				
۸	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**			■	تعداد نشست‌های همزمان کاربر در این محصول به صورت ثابت ۵ نشست است و در صورت وجود نشست‌های همزمان، این موضوع در قالب هشدار در پنل کاربری به کاربر اعلام می‌شود.
	در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشست‌های قبلی هنگام برقراری یک نشست جدید (به جزء مواردی که فعال بودن هم‌زمان چندین نشست موردنیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود.)	□		
		به‌روزرسانی اطلاعات پیشینه احراز هویت	□		
		سایر موارد	■		
۹	**محصول باید بر روی تغییرات مشخصه‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			□	در صورت ویرایش اطلاعات امنیتی کاربر فعال، نشست وی خاتمه می‌یابد.
	قوانینی که در صورت تغییر مشخصه‌های امنیتی کاربر فعال اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	□		
		سایر موارد	■		

۴/۲ حفاظت از داده کاربری

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

شماره الزام	کلاس حفاظت از داده کاربری					توضیحات
۱	**محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.**				■	موجودیت‌ها فعال سامانه عبارتند از کاربران شامل کاربر ارشد و دیگر کابران که کاربر عادی تلقی می‌شوند. موجودیت‌های غیرفعال سامانه عبارتند از، نمایشگرها، گروه نمایشگرها، برنامه‌های زمانبندی، چیدمان‌ها، گروه چیدمان‌ها، رکوردهای وضوح تصویر، محتواهای افزوده شده، تنظیمات و انواع گزارش‌ها. کنترل دسترسی کاربران در بخش مدیریت (Management) > کاربران (Users) در دسترس است و هر کاربر تنها قادر به مشاهده کابران زیرمجموعه خود است. همچنین هر کاربر می‌تواند اقدام به تعیین
	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	رکوردها، مستندات و فرا-داده[1]	■			
		داده متعلق به کاربران	■			
		داده احراز هویت	■			
		سایر موارد	■			

[1] Metadata

	می‌شوند، مشخص گردد.				سطح دسترسی کاربران زیرمجموعه خود به بخش‌ها مختلف سامانه نماید. این دسترسی حداکثر در حد دسترسی خود کاربر می‌تواند باشد. همچنین هر کاربر قادر به ایجاد، مشاهده، ویرایش و حذف موجودیت‌های غیرفعال خود و یا آن مواردی است که توسط کابران دیگر به وی دسترسی عمل مربوطه داده شده است. علاوه بر این موارد، کابر ارشد در بخش مدیریت (Management) > تنظیمات در تب اجازه دسترسی (Permissions) می‌تواند سیاست‌های اعمال دسترسی کاربران و نحوه صدور مجوزهای مربوطه را تعیین کند.
	عملیاتی که خط-مشی‌های 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 فرا-داده وابسته به موجودیت غیرفعال	■		
		سایر موارد	■		
۲	**محصول باید بر اساس مشخصه‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**			■	خط‌مشی‌های کنترلی علاوه بر مجوزهای اولیه کاربر که توسط مدیر وی به او تخصیص داده شده، براساس مجوزهای دسترسی داده شده توسط دیگر کاربران به وی برای دسترسی به موجودیت‌های غیر فعال اعمال می‌شوند.
	مشخصه‌هایی 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 کنترل شده را مجاز نماید (این قاعده**			■	برای هر موجودیت فعال این لیست دسترسی توسط کابر صاحب آن موجودیت با استفاده از دکمه اجازه

	می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد).			دسترسی (Permissions) قابل کنترل است و یا برای برخی موجودیت‌های غیرفعال مانند برنامه‌های زمانبندی، براساس سیات‌های تعیین شده توسط کاربر ارشد در بخش مدیریت (Management) > تنظیمات در تب اجازه دسترسی (Permissions) اعمال می‌شود.
۴	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			کنترل دسترسی براساس موارد عنوان شده در توضیح دو مورد قبلی اعمال می‌شود.
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[2] از پیش تعریف شده	☐	
		سایر موارد	■	
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.**		■	
۶	**محصول باید هنگام دریافت داده کاربری خطمشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی**		■	در این سامانه به دلیل نمایش محتوای تصویری، صوتی یا ویدئویی وجود Convertor داخلی برای این

[2] Threshold

	مرتبط با داده کاربری استفاده کند.				منظور، محدودیتی در حجم وجود ندارد و تنها برای جلوگیری از بارگزاری داده نامربوط، فرمت فایل‌ها محدود شده است.
	مشخصه‌های 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	☐		
		حجم و اندازه	☐		
		فرمت	■		
		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 دریافت شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.**			■	از طریق کانال امن TLS با استفاده از پروتکل HTTPS انجام می‌شود.
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☐	این سامانه جهت اطلاع رسانی عمومی انجام می‌شود. بنابراین خروج فایل همان نمایش فایل با استفاده از URL است که این امر برای همه آزاد است. تنها موضوع مهم دسترسی برای بارگزاری و تغییر فایل ها
	مشخصه‌های امنیتی مرتبط با داده	نوع داده	☐		
		حجم و اندازه	☐		

	کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	فرمت	☐		است که در الزامات قبلی به آن پرداخته شده است.
		سایر موارد	☐		
۹	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**			☐	این سامانه جهت اطلاع رسانی عمومی انجام می‌شود. بنابراین خروج فایل همان نمایش فایل با استفاده از URL است که این امر برای همه آزاد است. تنها موضوع مهم دسترسی برای بارگزاری و تغییر فایل ها است که در الزامات قبلی به آن پرداخته شده است.
	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج رکوردها را محدود نماید، به طوری‌که کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☐		
		سایر موارد	☐		
۱۰	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره شده در محصول تشخیص دهد**			■	
	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود	درهم شده[3] داده‌های کاربری ذخیره شده، نگهداری می‌شود	■		
		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	ایجاد هشدار/اخطار برای نقش‌های مجاز	☐		
		تصحیح داده بر اساس مقادیر قبل	☐		
		سایر موارد	☐		

[3] Hash

	(وجود یک مورد لازم و کافی است)				

۵/۲ مدیریت امنیت

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

شماره الزام	کلاس 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.**			■	تنظیمات سامانه تنها در اختیار کاربر ارشد است و امکان صدور مجوز دسترسی به این تنظیمات برای دیگر کاربران وجود ندارد.
	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 سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			■	کاربر ارشد می‌تواند در بخش مدیریت (Management) > تنظیمات (Settings) به تغییر تنظیمات پیشفرض سامانه بپردازد. همچنین امکان مدیریت و حذف کاربران زیرمجموعه

	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد	پرس‌وجو	☐		برای هر کاربر در بخش مدیریت (Management) > کاربران (Users) وجود دارد.
		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.**			■	کاربر ارشد می‌تواند موارد پیش‌فرض را در بخش مدیریت (Management) > تنظیمات (Settings) ویرایش کند. همچنین همه کاربران امکان ایجاد، مشاهده، ویرایش یا مقداردهی، پرس و جو و حذف داده های خود را دارند.
	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 این سامانه تنها کاربر ارشد امکان مشاهده داده‌های ممیزی را دارد. بنابراین موارد اول و دوم موضوعیت ندارند. رسیدن به حد آستانه و یا وقوع مشکل در عملیات ممیزی در قالب هشدار به کاربر ارشد اعلام می‌شود و تا رفع این مشکل، داده‌های ممیزی در syslog ذخیره خواهند شد.
	در صورتی که هر کدام از موارد مطرح شده، 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 رکوردهای ممیزی	☐		
		پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	☐		
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	■		

		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول در سمت پرتال، مصداق: غیرفعال کردن کاربر	■		هر کاربر می‌تواند در بخش مدیریت (Management) > کاربران (Users) اقدام به غیرفعال یا فعال کردن کاربران زیرمجموعه خود نماید. گزینه‌های مربوط به موارد "انتخاب زمان اجرای حفاظت از اطلاعات باقی‌مانده که می‌تواند در محصول قابل پیکربندی باشد. " و "ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول" در بخش مدیریت (Management) > تنظیمات (Settings) در دسترس کاربر ارشد است. هرگونه خطا در این سامانه توسط پیغام خطای مناسب به کاربر نمایش داده می‌شود و پیکربندی جهت انجام عملیات از پیش تعیین شده در این زمینه وجود ندارد. حد آستانه برای تلاش‌های ناموفق ورود در این سامانه مقدارثابت ۵ است. در هنگام شکست احراز هویت و رسیدن به حد آستانه ۵، کاربر برای ۵ دقیقه امکان تلاش برای ورود ندارد. مدیریت معیارها برای تنظیم کلمه عبور در بخش مدیریت (Management) > تنظیمات (Settings) در
		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 سمت پرتال بعنوان مثال سیاست گذرواژه	■		
		در نظر گرفتن یک عملیات از پیش تعیین شده 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 کلمات عبور	■		
		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 فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل	□		

		موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد. این محصول بصورت Identety Based می باشد و هر عملی بر حسب کاربر قابل شناسایی است			دسترس کاربر ارشد است. هر کاربر در بخش مدیریت (Management) > کاربران (Users) امکان مدیریت داده‌های احراز هویت کاربران زیرمجموعه خود را دارد. در این سامانه هیچ عملیاتی قبل از احراز هویت کاربر در دسترس نیست، بنابراین هیچ عملیاتی انجام نمی‌شود. مدیریت ساز و کارها و قوانین احراز هویت در بخش مدیریت (Management) > تنظیمات (Settings) در دسترس کاربر ارشد است. فرآیندهای احراز هویت در این سامانه فقط توسط کاربر ارشد قابل مدیریت است و دیگر کاربران تنها قادر به مدیریت کاربران زیرمجموعه خود هستند. تغییر مشخصه‌های امنیتی موجودیت‌های فعال در این سامانه تنها در بخش مدیریت (Management) > تنظیمات (Settings) در دسترس کاربر ارشد است. هر کاربر در بخش مدیریت (Management) > کاربران (Users) امکان کنترل دسترسی کاربران زیرمجموعه خود را در سطح برنامه دارد. تنها کاربر ارشد به عنوان نقش مشخص و از پیش
		مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت-های فعال پیش‌فرض را تعریف کند و تغییر دهد.	■		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول در سمت پرتال بعنوان مثال روتر مشتریان بصورت پیش فرض قابل تنظیم است	■		
		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. برای سرویس جلسات سازمانی زمان کاربرد ندارد، دلیلی برای فعال و غیر فعال کردن این سرویس ارتباطی که مانند تلفن می باشد بر حسب زمان وجود ندارد.	□		

					تعریف شده در این محصول وجود دارد. در خصوص دیگر کاربران، کاربر مدیر امکان تعریف سطح دسترسی کاربر زیرمجموعه خود را حداکثر در سطح دسترسی خود در بخش مدیریت (Management) > کاربران (Users) دارد. تعداد نشست‌های همزمان کاربر در این محصول به صورت ثابت ۵ نشست است و در صورت وجود نشست‌های همزمان، این موضوع در قالب هشدار در پنل کاربری به کاربر اعلام می‌شود. زمان مجاز غیرفعال بودن در این سامانه به صورت ثابت ۱۰ دقیقه است و پس از آن نشست کاربر خاتمه می‌یابد.
۵	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**			■	تنها کاربر ارشد به عنوان نقش مشخص و از پیش تعریف شده در این محصول وجود دارد. در خصوص دیگر کاربران، کاربر مدیر امکان تعریف سطح دسترسی کاربر زیرمجموعه خود را حداکثر در سطح دسترسی خود در بخش مدیریت (Management) > کاربران (Users) دارد.
	نقش‌هایی که در محصول پشتیبانی می‌شوند، مشخص گردد.	مدیر سیستم	□		
		کاربر پیشرفته	□		
		کاربر عادی	□		
		سایر موارد	■		
۶	**محصول باید قادر باشد کاربران را به نقش‌های تعریف شده یا قابل**			■	هر کاربر امکان تعریف سطح دسترسی کاربران

	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.		زیرمجموعه خود را حداکثر در سطح دسترسی خود در بخش مدیریت (Management) > کاربران (Users) دارد.

۶/۲ حفاظت از توابع امنیتی محصول

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

شماره الزام	کلاس حفاظت از توابع امنیتی محصول				توضیحات
۱	**محصول باید هنگام رخ دادن هرگونه شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.**	■			
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد	شکست‌های نرم‌افزاری	■		
		شکست‌های سخت‌افزاری	□		

۲	**محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی محافظت از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.**		■	
۳	**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 محصول پشتیبانی می‌شوند، مشخص گردد.	داده‌های احراز هویت	■	
		کلید	□	
		امضای دیجیتال	□	
		داده‌های ممیزی	□	
		سایر موارد	□	
۴	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی معتبر، تولید یا استفاده نماید.**		■	این محصول بر روی سیستم‌عامل لینوکس نصب و راه‌اندازی می‌شود.
	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 به‌روزرسانی نرم‌افزار و میان‌افزار محصول را**		■	بروزرسانی این محصول توسط توسعه دهنده و به

	برای مدیر سیستم فراهم نماید.				صورت دستی انجام می‌شود.
	روش به‌روزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروز رسانی دستی	■		
		جستجوی خودکار به‌روزرسانی‌ها	□		
		به‌روزرسانی‌های خودکار	□		
		به‌روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی	□		
۶	**در صورت استفاده از به‌روزرسانی به روش خودکار، محصول باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**			□	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت‌سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضاء دیجیتال	□		
		درهم‌ساز منتشرشده	□		

۷٫۲ تخصیص منابع

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

شماره	کلاس تخصیص منابع	توضیحات

الزام			
۱	**محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.**	■	

۸/۲ دسترسی به محصول

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

شماره الزام	کلاس دسترسی محصول		توضیحات
۱	**محصول باید حداکثر تعداد نشست‌های هم‌زمان متعلق به یک کاربر را محدود نماید.**	■	تعداد نشست‌های همزمان کاربر در این محصول به صورت ثابت ۵ نشست است و در صورت وجود نشست‌های همزمان، این موضوع در قالب هشدار در پنل کاربری به کاربر اعلام می‌شود.
۲	**محصول باید کلیه نشست‌های تعاملی راه‌دور[۴] 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**	■	

[4]Remote

	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 ■	■	علاوه بر نمایش تاریخ و ساعت آخرین تلاش موفق در قالب Notification، برای خوانایی و سادگی، با نگه داشتن اشاره‌گر بر روی این Notification، آدرس IP کلاینتی که این تلاش با آن انجام شده نیز به کاربر نمایش داده می‌شود.
۵	**در صورت برقراری نشست به طور موفقیت‌آمیز، 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 ■	■	علاوه بر نمایش تاریخ و ساعت آخرین تلاش ناموفق در قالب Notification، برای خوانایی و سادگی، با نگه داشتن اشاره‌گر بر روی این Notification، آدرس IP کلاینتی که این تلاش با آن انجام شده نیز به کاربر نمایش داده می‌شود.
۶	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**	■	
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.** پارامترهای موجود برای جلوگیری از مکان □ شماره پورت □	□	

	نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	روز	☐		
		زمان	☐		
		سایر موارد	☐		

۹/۲ کانال‌ها/مسیرهای مورد اعتماد

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

شماره الزام	کلاس 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 داده و از تغییر و افشاء داده تبادلی حفاظت نموده و تغییرات را تشخیص دهد.** **در صورت انتخاب مورد HTTPS، رعایت الزام ۳.۱ و در صورت انتخاب TLS، رعایت الزامات ۳.۲ تا ۳.۴ که در بخش ۳ بیان گردیده است،**	■	

	الزامی است.			
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	■	
		TLS	□	
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. برای مثال اگر در الزامات مربوط به کلاس کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

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	**درصورتی‌که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (در هنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید.** **اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۳.۵ انجام می‌شود که در این صورت الزامات بخش ۳.۵ الزامی است.**			□	این محصول تحت وب است.
		محصول تنها از موارد بیان شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	□	
			برای برقراری اتصال درخواست مجوز کند.	■	

۲/۳ پروتکل TLS Client

شماره الزام	پروتکل TLS Client			توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.**		■	در سرور این سامانه از TLS نسخه 1.2 استفاده شده است.
	مجموعه رمز مورد استفاده و پیاده‌سازی شده در محصول، انتخاب گردد.	TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	■	
		TLS_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268	□	
		TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268	■	
		TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	■	
		TLS_DHE_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268	□	
		TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268	■	
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492	■	
		TLS_ECDHE_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 4492	□	
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492	■	
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492	□	

		☐	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		■	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256 مطابق با RFC 5246		
		■	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
		☐	TLS _RSA_WITH_AES_192_GCM_ SHA256 مطابق با RFC 5288		
		■	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		

		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق باRFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289		
۲	**محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید 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.**			■	این محصول تحت وب است.
		در صورت	ارتباط را برقرار نکند	☐	

	پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	برای برقراری ارتباط درخواست مجوز کند	■		
		سایر موارد	□		
۴	**محصول باید در پیام ClientHello برای استفاده از منحنی‌ها، بر اساس موارد زیر عمل نماید.**			□	
	در صورتی که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.	Supported Elliptic Curves Extension را ارائه نکند.	□		
		Supported Elliptic Curves Extension را به همراه NIST curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.	■		
		هیچ منحنی دیگری	□		

۳٫۳ پروتکل TLS Server

شماره الزام	پروتکل TLS Server			توضیحات
۵	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.**		■	
		TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	■	

		■	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268		
		■	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268		
		■	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		
		■	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		□	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		
		□	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		■	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		■	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		□	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		□	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
		□	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		

		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		■	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
۶	**محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0و TLS1.1 دارند را رد نماید.**			■	
۷	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			■	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	■	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت		
		■	پارامترهای ECDH با استفاده از NIST curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگری		
		■	پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت		

۴/۳ 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	**محصول در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده[5] کلاینت مورد انتظار بوده است، نباید کانال امن را برقرار سازد.**	☐	

۵٫۳ اعتبارسنجی گواهی‌نامه

شماره الزام	شناسایی و احراز هویت			توضیحات
۳	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند.**	☐		
	تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.		☐	
	مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.		☐	
	محصول باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.		■	

[5] Identifier

	روش‌های تائید وضعیت فسخ گواهی‌نامه	■	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 696		
		☐	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶.۳		
		☐	فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵		
		☐	هیچ روش فسخ دیگری		
	قوانین تائید فیلد extendedKeyUsage	☐	گواهی‌نامه‌های مورداستفاده برای تائید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند		
		☐	گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف " Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف Client "Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.		
۴	**محصول باید تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.**		☐		
۵	**محصول باید جهت پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های**		■		

	X.509v3 تعریف‌شده در RFC 5280 استفاده کند.				
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.	HTTPS	■		
		TLS	☐		
		امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم	☐		
		امضای کد برای تائید یکپارچگی	☐		
		سایر موارد	☐		