به نام خدا

سند هدف امنیتی

شهرسازی - نسخه 1402.03.10.01

تحلیلگران آمارد نوین آمل

1402.03

نسخه 1.7

فهرست

[1- معرفی سند هدف امنیتی 5](#_Toc138771693)

[1-1- مرجع سند هدف امنیتی 5](#_Toc138771694)

[1-2- مرجع هدف ارزیابی 5](#_Toc138771695)

[1-3- مرور كلی هدف ارزیابی 5](#_Toc138771696)

[1-3-1- توابع امنیتی اصلی هدف ارزیابی 5](#_Toc138771697)

[1-3-2- نوع هدف ارزیابی 7](#_Toc138771698)

[1-3-3- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی 7](#_Toc138771699)

[1-4- توصیف هدف ارزیابی 7](#_Toc138771700)

[1-4-1- حوزه فیزیکی 7](#_Toc138771701)

[1-4-2- حوزه منطقی 8](#_Toc138771702)

[2- ادعای انطباق 10](#_Toc138771703)

[2-1- انطباق با استاندارد ارزیابی امنیتی معیار مشترک 10](#_Toc138771704)

[2-2- انطباق با پروفایل حفاظتی 10](#_Toc138771705)

[2-3- انطباق با سطح تضمین امنیتی 10](#_Toc138771706)

[3- تعریف مسائل امنیتی 10](#_Toc138771707)

[3-1- خطمشی 10](#_Toc138771708)

[3-2- تهدیدات 11](#_Toc138771709)

[3-3- فرضیات 12](#_Toc138771710)

[4- اهداف امنیتی 13](#_Toc138771711)

[4-1- اهداف امنیتی برای هدف ارزیابی 13](#_Toc138771712)

[4-2- اهداف امنیتی برای محیط عملیاتی 15](#_Toc138771713)

[5- نیازمندی‌‌های امنیتی 17](#_Toc138771714)

[5-1- الزامات کارکرد امنیتی 17](#_Toc138771715)

[5-1-1- کلاس ممیزی امنیت 21](#_Toc138771716)

[5-1-2- کلاس پشتیبانی از رمزنگاری 29](#_Toc138771717)

[5-1-3- کلاس شناسایی و احرازهویت 31](#_Toc138771718)

[5-1-4- کلاس حفاظت از داده کاربری 36](#_Toc138771719)

[5-1-5- کلاس مدیریت امنیت 40](#_Toc138771720)

[5-1-6- کلاس حفاظت از توابع امنیتی هدف ارزیابی 45](#_Toc138771721)

[5-1-7- کلاس دسترسی به هدف ارزیابی 47](#_Toc138771722)

[5-1-8- كلاس كانال‌ها و مسیر‌‌های مورد اعتماد 48](#_Toc138771723)

[5-1-9- كلاس تخصیص منابع 49](#_Toc138771724)

[5-2- توجیهات 51](#_Toc138771725)

[5-3- الزامات تضمین امنیتی 51](#_Toc138771726)

[6- خلاصه مشخصات هدف ارزیابی 52](#_Toc138771727)

[**تولید داده ممیزی** 52](#_Toc138771728)

[**بازبینی داده‌های ممیزی** 52](#_Toc138771729)

[**انتخاب داده‌های ممیزی** 53](#_Toc138771730)

[**ذخیره رویدادهای ممیزی** 53](#_Toc138771731)

[**ازبین‌رفتن داده‌های ممیزی** 54](#_Toc138771732)

[**عملیات رمزنگاری** 54](#_Toc138771733)

[**خط‌مشی و عملیات مهار دسترسی** 55](#_Toc138771734)

[**ورود داده کاربری به محصول با مشخصه امنیتی** 55](#_Toc138771735)

[**خروج داده کاربری به محصول با مشخصه امنیتی** 56](#_Toc138771736)

[**صحت داده کاربری ذخیره‌شده** 56](#_Toc138771737)

[**مدیریت احراز هویت ناموفق** 57](#_Toc138771738)

[**تعریف مشخصات کاربر** 57](#_Toc138771739)

[**مدیریت کلمه عبور** 58](#_Toc138771740)

[**احراز هویت کاربر** 58](#_Toc138771741)

[**سازوکار احراز هویت چندگانه** 59](#_Toc138771742)

[**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر** 59](#_Toc138771743)

[**مدیریت مشخصه‌های امنیتی** 60](#_Toc138771744)

[**حفظ وضعیت امن در زمان شکست و تحمل خطا** 60](#_Toc138771745)

[**محدودیت برروی چندین نشست هم‌زمان** 61](#_Toc138771746)

[**خاتمه دادن به نشست‌ها** 61](#_Toc138771747)

[**سوابق دسترسی به محصول** 62](#_Toc138771748)

[**سوابق دسترسی به محصول** 62](#_Toc138771749)

[**برقراری نشست** 63](#_Toc138771750)

# معرفی سند هدف امنیتی

در راستای ارزیابی امنیتی محصوالت مبتنی بر معیار مشترک الزم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصوالت این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه شدهاند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطالعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد 1R4. V3 15408 ISO/IRISI در راستای این هدف تهیه نموده است. این پروفایل حفاظتی، به بیان الزامات نرم افزار شهرسازی آمارد می‌پردازد.

## مرجع سند هدف امنیتی

|  |  |
| --- | --- |
| عنوان سند هدف امنیتی | ST-Shahrsazi-Amard |
| نسخه | 1.7 |
| تاریخ | 1402.03.08 |
| نویسندگان | سیدرسول حسینی |

## مرجع هدف ارزیابی

|  |  |
| --- | --- |
| نام تولید کننده (شرکت) | تحلیلگران آمارد |
| نام محصول | شهرسازی |
| نوع محصول | وب |
| نسخه | 1402.03.10.01 |

## مرور كلی هدف ارزیابی

### توابع امنیتی اصلی هدف ارزیابی

**احرازهویت و مجوزدهی:** عملیات احراز هویت و مجوزدهی باید به طور موثری انجام شود. احرازهویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌­گیرد. لازم به ذکر است برای مدیریت کلمه عبور­‌های مورد استفاده باید روال‌‌های امن وجود داشته باشد. در صورتیکه محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احرازهویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می‌­شود. از جمله سازوکار­‌های احراز هویت می‌­توان به وارسی نام کاربری و کلمه عبور، وارسی SMS، احراز هویت از طریق یک برنامه موبایل، وارسی بیومتریک و توکن سخت‌افزاری اشاره نمود.

**کنترل دسترسی:** محصول، قابلیت­‌های لازم برای محدود کردن دسترسی را دارد، بطوریکه تنها موجودیت­‌های مجاز، دارای دسترسی به داده و کارکرد‌های محصول هستند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌­گیرد. محصول ممکن است همچنین آدرس­‌های IP اتصالات فعال را کنترل نماید، و تنها به آدرس­‌های IP از پیش تعریف شده در یک بازه زمانی خاص برای عملیات­‌های حساس اجازه اتصال دهد.

**ممیزی:** محصول به صورت خودکار، رکورد‌های ممیزی را به منظور ردیابی و کنترل فعالیت­‌های کاربر بر روی دارایی­ها، تغییرات کنترل دسترسی و پیکربندی جمع­آوری می‌­نماید. محتوای رکورد‌های ممیزی، روش­‌های حفظ رکورد و فواصل نگهداری را می‌­توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکورد‌های ممیزی را ندارند.

**مدیریت:** محصول، برای مدیریت کاربران و دسترسی‌ها واسط­‌های مدیریتی لازم را فراهم می‌­نماید. سرعت و دقت این واسط­ها در تصمیم­گیری در طول یک رخداد امنیتی بسیار مهم است.

**صحت رکوردها و بررسی منابع:** حذف یا تغییر هر رکورد توسط محصول مجاز نمی­باشد. بنابراین، دسترسی و تغییر سند و/یا فرا داده[[1]](#footnote-1) آن باید محدود گردد. صحت رکورد‌های ذخیره شده، توسط روشی مانند امضای دیجیتال مهیا می‌­گردد.

**پشتیبان‌گیری:** عملیات پشتیبان‌گیری بر روی داده، مستندات و رکورد‌های ممیزی که محصول از آنها محافظت می‌­نماید، می‌­تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌­گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌­دهد.

**کنترل گردش مستندات و اطلاعات:** حداکثر اندازه فایل می‌­تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره سازی را در نظر گرفته و در برابر سرریز ذخیره­سازی اقدامات احتیاطی لازم را اتخاذ می‌­نماید. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

**درهم­سازی/رمز نمودن داده حساس:** مثالی از داده حساس­ کلمه­‌های عبور یا رکورد‌های محرمانه می‌­باشد. داده حساس بر روی محصول به صورت واضح ذخیره نمی شوند و با سازوکاری از آنها حفاظت می‌شود. همچنین باید رکورد‌های محرمانه به صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهمسازی و رمزنگاری انتخاب شده باید به اندازه کافی قوی باشد طوری­که توسط فناوری­‌های امروزی در یک بازه­ی منطقی قابل شکسته شدن نباشد.

### نوع هدف ارزیابی

سامانه شهرسازی، از نوع برنامه کاربردی تحت وب می‌باشد.

### نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

در جدول زیر سخت­افزار، نرم افزار و می‌ان افزار‌های لازم برای کارکرد محصول بیان شده است:

| کامپوننت­ها | حداقل الزامات |
| --- | --- |
| ماژول اصلی نرم افزار | * Windows Server 2022 * 8 GB Ram * 200 GB Free Space * Xeon 2650 CPU (4 core) * . Net Framework 4.8 |
| زیر سیستم GIS | * Windows Server 2016 * 8 GB Ram * 100 GB Free Space (SSD) * Xeon 2650 CPU (4 core) * Arc Gis 2016 |

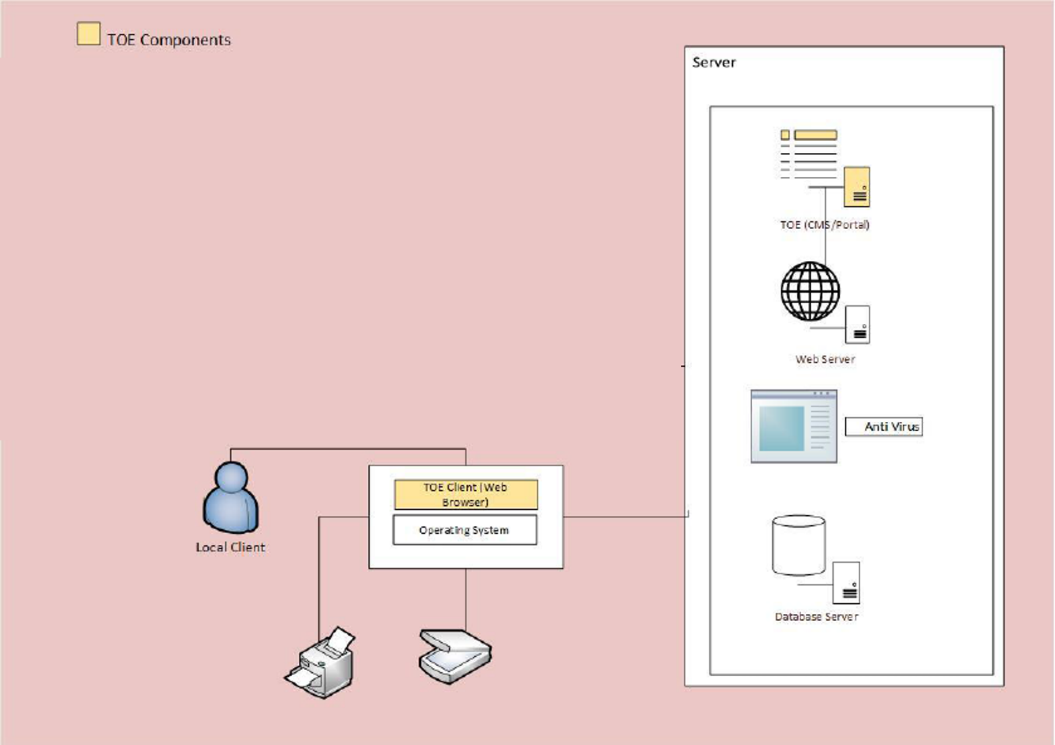
## توصیف هدف ارزیابی

### حوزه فیزیکی

عناصر سخت­افزاری و نرم­افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌­شود:

| عناصر محصول | شماره مدل یا نسخه |
| --- | --- |
| Web Application Framework | Microsoft ASP. NET MVC 5 / .Net Framework 4. 8 |
| Operation System | Microsoft Windows Server 2016 |
| Programming languages | C# |
| Relational Database Management System | Microsoft SQL Server 2016 |
| Software Development IDE for Application | Visual Studio 2022 |
| Source code management, Requirements management, Project management, Automated builds | GitLab |
| Web Server | IIS |
| Asynchronous Notifications to Client-Side Technology | Signal-R |
| . NET Platform Reporting Component | Stimul |

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



### حوزه منطقی

کارکرد‌های امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌­شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.

**احرازهویت و مجوزدهی:** عملیات احراز هویت و مجوزدهی باید به صورت اثرگذاری انجام شود. احرازهویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌گیرد. الزم به ذکر است برای مدیریت کلمه عبور‌های مورد استفاده باید روال‌های امن وجود داشته باشد. در صورتیکه محصول به سطح باالیی از امنیت نیاز داشته باشد، از یک سازوکار احرازهویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می‌شود. از جمله سازوکار‌های احراز هویت می‌توان به وارسی نام کاربری و کلمه عبور، وارسی SMS،احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، وارسی بیومتریک و توکن سختافزاری اشاره نمود.

**کنترل دسترسی:** محصول قابلیت محدود کردن دسترسی را دارد؛ بطوریکه تنها موجودیت‌های مجاز، امکان دسترسی به داده و کارکرد‌های محصول را دارا هستند. برای کاربران مجاز، کنترل دسترسی معموالً با استفاده از داده احراز هویت انجام می‌گیرد. همچنین محصول ممکن است آدرس‌هایIP اتصاالت فعال را کنترل نماید، و تنها به آدرس‌هایIP از پیش تعریف شده در یک بازه زمانی خاص برای عملیات‌های حساس اجازه اتصال دهد.

**ممیزی:** محصول به صورت خودکار، رکورد‌های ممیزی را به منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی ها، تغییرات کنترل دسترسی و پیکربندی جمع آوری می‌نماید. محتوای رکورد‌های ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکورد‌های ممیزی را ندارند.

**مدیریت:** محصول، برای مدیریت کاربران و دسترسیها واسط‌های مدیریتی الزم را فراهم می‌نماید. سرعت و دقت این واسط‌ها در تصمیم گیری در طول یک رخداد امنیتی بسیار مهم است.

**صحت رکوردها و بررسی منابع:** حذف یا تغییر هر رکورد توسط محصول مجاز نمیباشد. بنابراین، دسترسی و تغییر سند و/یا فرا داده آن باید محدود گردد. صحت رکورد‌های ذخیره شده، توسط روشی مانند امضای دیجیتال فراهم می‌گردد.

**پشتیبان گیری:** عملیات پشتیبان گیری بر روی داده، مستندات و رکورد‌های ممیزی که محصول از آنها محافظت می‌نماید، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

**کنترل گردش مستندات و اطلاعات:** حداکثر اندازه فایل می‌تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره سازی را در نظر گرفته و در برابر سرریز ذخیره سازی اقدامات احتیاطی الزم را اتخاذ می‌نماید. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

**درهمسازی/رمز نمودن دادهی حساس:** مثالی از داده‌ی حساس کلمه‌های عبور یا رکورد‌های محرمانه می‌باشد. داده‌ی حساس بر روی محصول به صورت واضح ذخیره نمی شوند و با سازوکاری از آنها حفاظت می‌شود. همچنین باید رکورد‌های محرمانه به صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهمسازی و رمزنگاری انتخاب شده باید به اندازه کافی قوی باشد طوریکه توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

# ادعای انطباق

## انطباق با استاندارد ارزیابی امنیتی معیار مشترک

|  |  |
| --- | --- |
| **انطباق با استاندارد ارزیابی امنیتی معیار مشترک** | ISO/IEC 15408, version 3.1, revision 5, April 2017 |
| **انطباق با SFRها (قسمت دوم از CC)** | توسعه یافته |
| **انطباق با SARها (قسمت سوم از CC)** | منطبق |

## انطباق با پروفایل حفاظتی

|  |  |
| --- | --- |
| نام پروفایل حفاظتی | "برنامه‌های کاربردی تحت شبکه نسخه 1.1 اسفندماه 96" |

## انطباق با سطح تضمین امنیتی

|  |  |
| --- | --- |
| سطح تضمین امنیتی | EAL1 |

# تعریف مسائل امنیتی

## خط­مشی

| خطمشی­ | توصیف |
| --- | --- |
| P. COMPLEMENTARY\_AUDIT | تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محفاظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می‌گیرند**.** |
| P. PROPER\_CONFIGURATION | پیکربندی پیشفرض محصول و مولفه‌‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامتر‌های پیکربندی همچون دایرکتوری root پیشفرض، خطا‌های پیشفرض و صفحات 404، مقادیر احراز هویت پیشفرض، نام کاربری پیشفرض، پورت‌های پیشفرض، صفحات پیشفرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خطمشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامتر‌های پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود. |
| P. E\_SIGNATURE | امضای دیجیتال مورد استفاده باید مطابق با استاندارد‌های مورد تائید موجود باشد. |

## تهدیدات

| تهدید | توصیف |
| --- | --- |
| T. UNAUTHORIZED\_ACCESS | مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد.  مهاجم می‌تواند با سود بردن از نقض‌های امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم می‌تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد.  این داده‌ها می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود. |
| T. DATA\_ALTERATION | رکوردها، مستندات و داده‌های حفاظت شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نمی باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید. |
| T. REPUDIATION | یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می‌باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از رکورد‌های ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه نمودن تعداد رکورد‌های بالا یا رکورد‌های غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید. |
| T. DATA\_DISCLOSURE | داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامتر‌های کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد |
| T. DENIAL\_OF\_SERVICE | مهاجم می‌تواند سبب گردد محصول در یک بازه‌ی زمانی، غیر قابل دسترسی یا بدون استفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوریکه محصول قادر به پاسخ نخواهد بود.  نوع ساد‌ه‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص می‌باشد که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته تر حمله DDoS می‌باشد که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد. |
| T. HARMFUL\_DATA | مهاجم می‌تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم می‌تواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکرد‌های محصول دسترسی یابد. |
| **T. ELEVATION\_OF\_PRIVILEGES** | مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید. |
| T. NETWORK\_EAVESDROP | در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده‌های تبادل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال می‌توان به موردی اشاره کرد که در آن یک کاربر تلاش می‌کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد نماید. |

## فرضیات

| فرضیه | توصیف |
| --- | --- |
| **A. TRUSTED\_ADMIN** | فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیدهاند و قوانین را دنبال می‌نمایند. |
| **A. TRUSTED\_DEVELOPER** | فرض شده است که افراد مسئول توسعه محصول )همانند برنامه نویس، طراح، غیره( افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند. |
| **A. EXPERIENCED\_ DEVELOPER** | فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکار‌های لازم برای مقابله با تمام آسیب پذیری‌های شناخته شده را اتخاذ می‌نمایند. |
| **A. SECURE\_ENVIRONMENT** | فرض شده است که تمام پیشبینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکورد‌های دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت می‌گیرد. |
| **A. PROPER\_BACKUP** | فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مولفه‌های سختافزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داد‌های از دست نمی رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی دهد. |
| **A. COMMUNICATION** | جهت ارتباط با نهاد‌های خارجی که » توابع امنیتی محصول « فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورد استفاده تحت حفاظت توابع محصول نیستند؛ به طور مناسبی درقبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند. |
| **A. SECURE\_DELIVERY** | فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهاد‌های مطمئن و واجد شرایط صورت می‌گیرد |
| **A. DIST\_DENIAL\_OF\_SERVICE** | فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود. |

# اهداف امنیتی

## اهداف امنیتی برای هدف ارزیابی

| هدف امنیتی | توصیف |
| --- | --- |
| **O. AUDIT** | 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. |
| **O. AUTH** | 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 کلمه‌های عبور قدرتمند نماید. محصول باید اجازه طبقهبندی رکوردها و مستندات را دهد و با توجه به طبقهبندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکورد‌های شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تالش است تا از تهدیدی چون رسیدن به سطح دسترسی باالتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید مدیر سیستم را با استفاده از سازوکار‌های قویتری احرازهویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP،محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود. |
| **O. DATA\_FLOW\_CONTROL** | محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنج IP تعریف شده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکار‌های فیلترینگ استفاده نماید. |
| **O. DATA\_INTEGRITY** | محصول باید نسبت به صحت داده ممیزی و دادهی رکورد با تشخیص هرگونه تغییر بر روی این دادهها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات الزم را انجام دهد. |
| **O. MANAGEMENT** | محصول باید تمام کارکردها را برای مدیر سیستم به منظور مدیریت امن و کارامد سیستم فراهم نماید. محصول باید سازوکار‌های کنترل دسترسی مناسبی جهت حفاظت از واسط‌های مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش‌های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید. |
| **O. ERROR\_MANAGEMENT** | محصول باید صورت امن و کارامد سازوکار مدیریت خطا را فراهم نماید. خطا‌های رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطالعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطالعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید. |
| **O. RESIDUAL\_DATA\_MNG** | محصول باید اطمینان دهد که هر دادهی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می‌گردد. |
| **O. TLS\_COMMUNICATION** | تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند. |

## اهداف امنیتی برای محیط عملیاتی

| هدف امنیتی | توصیف |
| --- | --- |
| **OE. SECURE\_ENVIRONMENT** | محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مولفهها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکار‌های حفاظتی می‌توان به غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود. |
| **OE. COMMUNICATION** | محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن فراهم گردد |
| **OE. TRUSTED\_ADMIN** | محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکرد‌های محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند. |
| **OE. TRUSTED\_DEVELOPER** | محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند. |
| **OE. EXPERIENCED\_DEVELOPER** | محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهندهی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابل‌های الزم برای تمام آسیبپذیری‌های امنیتی شناخته شده را در نظر می‌گیرد. |
| **OE. COMPLEMENTARY\_AUDIT** | محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می‌باشد. رکورد‌های ممیزی محصول در صورت ترکیب با باقی رکورد‌های ممیزی بسیار معنادار خواهند بود. |
| **OE. SECURE\_DELIVERY** | تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. عالوه بر این، کارکردها و/یا پارامتر‌های استفاده شده به منظور تست باید پاک یا غیر قابل دسترس گردند. |
| **OE. PROPER\_BACKUP** | نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال‌های از پیش تعریف شده استفاده گردد. همچنین باید از واحد‌های ذخیره سازی و دیگر مولفه‌های سختافزاری نیز نسخه پشتیبان تهیه گردد. |

# نیازمندی‌‌های امنیتی

## الزامات کارکرد امنیتی

الزامات مندرج در اين بخش از پروفايل حفاظتی مرجع آورده شده اند.

در سند جاری کلیه عملگر‌های انتخاب به صورت زیرخط دار و عملگر‌های اختصاص به صورت **بولد** نوشته شده اند و براکت‌ها نیز برای عملگرها لحاظ شده است.

| شماره المان | نام كلاس | نام المان | تطابق الزام با استاندارد |
| --- | --- | --- | --- |
|  | **ممیزی امنیت** | **تولید داده ممیزی 1** | FAU\_GEN.1.1 |
|  | **تولید داده ممیزی 2** | FAU\_GEN.1.2 |
|  | **مرتبط نمودن هویت کاربر به رویداد 1** | FAU\_GEN.2.1 |
|  | **بازبینی داده ممیزی 1** | FAU\_SAR.1.1 |
|  | **بازبینی داده ممیزی 2** | FAU\_SAR.1.2 |
|  | **بازبینی داده ممیزی 3** | FAU\_SAR.2.1 |
|  | **بازبینی داده ممیزی 4** | FAU\_SAR.3.1 |
|  | **ذخیره سازی رویداد‌های ممیزی 1** | FAU\_STG.1.1 |
|  | **ذخیره سازی رویداد‌های ممیزی 2** | FAU\_STG.1.2 |
|  | **ذخیره سازی رویداد‌های ممیزی 6** | FAU\_STG.3.1 |
|  | **ذخیره سازی رویداد‌های ممیزی 7** | FAU\_STG. 4.1 |
|  | **انتخاب داده ممیزی 1** | FAU\_SEL.1.1 |
|  | **پشتیبانی از رمز‌نگاری** | **عملیات رمزنگاری 1 (1)** | FCS\_COP.1.1(1) |
|  | **عملیات رمزنگاری 1 (2)** | FCS\_COP.1.1(2) |
|  | **الزامات پروتکل TLS Client (1)** | FCS\_TLSC\_EXT.1.1 |
|  | **الزامات پروتکل TLS Client (2)** | FCS\_TLSC\_EXT.1.2 |
|  | **الزامات پروتکل TLS Client (3)** | FCS\_TLSC\_EXT.1.3 |
|  | **الزامات پروتکل TLS Client (4)** | FCS\_TLSC\_EXT. 4.1 |
|  | **الزامات پروتکل HTTPS** | FCS\_HTTPS\_EXT.1 |
|  | **الزامات پروتکل HTTPS (1)** | FCS\_HTTPS\_EXT.1.1 |
|  | **الزامات پروتکل HTTPS (2)** | FCS\_HTTPS\_EXT.1.2 |
|  | **الزامات پروتکل HTTPS (3)** | FCS\_HTTPS\_EXT.1.3 |
|  | **شناسایی و احرازهویت** | **مدیریت کلمه عبور 1** | FIA\_PMG\_EXT.1.1 |
|  | **مدیریت احراز هویت ناموفق 1** | FIA\_AFL.1.1 |
|  | **مدیریت احراز هویت ناموفق 2** | FIA\_AFL.1.2 |
|  | **تعریف مشخصات کاربر 1** | FIA\_ATD.1.1 |
|  | **احرازهویت کاربر1** | FIA\_UAU.1.1 |
|  | **احرازهویت کاربر2** | FIA\_UAU.1.2 |
|  | **احراز هویت کاربر 7** | FIA\_UAU. 5.1 |
|  | **احراز هویت کاربر 8** | FIA\_UAU. 5.2 |
|  | **انقیاد مشخصه‌های امنیتی کاربربا موجودیت فعال متناظر 1** | FIA\_USB.1.1 |
|  | **انقیاد مشخصه‌های امنیتی کاربربا موجودیت فعال متناظر 2** | FIA\_USB.1.2 |
|  | **انقیاد مشخصه‌های امنیتی کاربربا موجودیت فعال متناظر 3** | FIA\_USB.1.3 |
|  | **شناسایی کاربر 1** | FIA\_UID.1.1 |
|  | **شناسایی کاربر 2** | FIA\_UID.1.2 |
|  | **الزامات پروتکلX509 (1)** | FIA\_X509\_EXT.1.1 |
|  | **الزامات پروتکلX509 (2)** | FIA\_X509\_EXT.1.2 |
|  | **الزامات پروتکلX509 (3)** | FIA\_X509\_EXT.2.1 |
|  | **الزامات پروتکلX509 (4)** | FIA\_X509\_EXT.2.2 |
|  | **حفاظت از داده کاربری** | **حفاظت از اطلاعات باقیمانده در منابع 2** | FDP\_RIP.2.1 |
|  | **ورود داده‌های کاربری به محصول 4** | FDP\_ITC.2.1 |
|  | **ورود داده‌ کاربری به محصول با مشخصه امنیتی 2** | FDP\_ITC.2.2 |
|  | **ورود داده‌های کاربری به محصول 6** | FDP\_ITC.2.3 |
|  | **ورود داده‌های کاربری به محصول 7** | FDP\_ITC.2. 4 |
|  | **ورود داده‌های کاربری به محصول 8** | FDP\_ITC.2. 5 |
|  | **صحت داده‌های کاربری ذخیره شده 2** | FDP\_SDI.2.1 |
|  | **صحت داده‌های کاربری ذخیره شده 3** | FDP\_SDI.2.2 |
|  | **خط مشی کنترل دسترسی 1** | FDP\_ACC.1.1 |
|  | **عملیات کنترل دسترسی 1** | FDP\_ACF.1.1 |
|  | **عملیات کنترل دسترسی 2** | FDP\_ACF.1.2 |
|  | **عملیات کنترل دسترسی 3** | FDP\_ACF.1.3 |
|  | **عملیات کنترل دسترسی 4** | FDP\_ACF.1. 4 |
|  | **مدیریت امنیت** | **مدیریت کارکرد در محصول 1** | FMT\_MOF.1.1 |
|  | **مدیریت مشخصه‌های امنیتی 1** | FMT\_MSA.1.1 |
|  | **مدیریت مشخصه‌های امنیتی 3** | FMT\_MSA.3.1 |
|  | **مدیریت مشخصه‌های امنیتی 4** | FMT\_MSA.3.2 |
|  | **مدیریت داده‌های محصول 1 – مدیر سیستم** | FMT\_MTD.1.1(1) |
|  | **مدیریت داده‌های محصول 1 – کاربران عادی** | FMT\_MTD.1.1(2) |
|  | **کارکرد‌های مدیریتی محصول 1** | FMT\_SMF.1.1 |
|  | **نقش‌های امنیتی 1** | FMT\_SMR.1.1 |
|  | **نقش‌های امنیتی 2** | FMT\_SMR.1.2 |
|  | **حفظ وضعیت امن در زمان شکست 1** | FPT\_FLS.1.1 |
|  | **سازگاری داده‌های امنیتی بین محصول و مجودیت امن 1** | FPT\_TDC.1.1 |
|  | **سازگاری داده‌های امنیتی بین محصول و مجودیت امن 2** | FPT\_TDC.1.2 |
|  | **انتقال داده امنیتی در داخل محصول 1** | FPT\_ITT.1.1 |
|  | **مهر‌های زمانی 1** | FPT\_STM.1.1 |
|  | **دسترسی به محصول** | **مدیریت بر روی چندین نشست هم زمان 1** | FTA\_MCS.1.1 |
|  | **مدیریت بر روی چندین نشست هم زمان 2** | FTA\_MCS.1.2 |
|  | **قفل کردن و خاتمه دادن به نشست‌ها 5** | FTA\_SSL.3.1 |
|  | **قفل کردن و خاتمه دادن به نشست‌ها 6** | FTA\_SSL. 4.1 |
|  | **سوابق دسترسی به محصول 1** | FTA\_TAH.1.1 |
|  | **سوابق دسترسی به محصول 2** | FTA\_TAH.1.2 |
|  | **سوابق دسترسی به محصول 3** | FTA\_TAH.1.3 |
|  | **برقراری نشست 1** | FTA\_TSE.1.1 |
|  | **كانال‌ها و مسیر‌‌های مورد اعتماد** | **کانال امن 1** | FTP\_ITC.1.1 |
|  | **کانال امن 2** | FTP\_ITC.1.2 |
|  | **کانال امن 3** | FTP\_ITC.1.3 |
|  | **مسیر امن 1** | FTP\_TRP.1.1 |
|  | **مسیر امن 2** | FTP\_TRP.1.2 |
|  | **مسیر امن 3** | FTP\_TRP.1.3 |
|  | **تخصیص منابع** | **تحمل خطای 1** | FRU\_FLT.1.1 |
|  | **الزامات پیوست یک** | **(2) عملیات رمزنگاری 1-رمزنگاری و رمزگشایی** | FCS\_COP.1.1(3) |
|  | **(4) عملیات رمزنگاری** | FCS\_COP.1.1(4) |
|  | **تولید کلید رمزنگاری** | FCS\_CKM.1.1 |
|  | **مدیریت کلید رمزنگاری** | FCS\_CKM\_EXT. 4.1 |
|  | **الزامات پروتکل TLS Server / احراز هویت** | FCS\_TLSS\_EXT.1.1 |
|  | **الزامات پروتکل TLS Server / احراز هویت** | FCS\_TLSS\_EXT.1.2 |
|  | **الزامات پروتکل TLS Server / احراز هویت** | FCS\_TLSS\_EXT.1.3 |

### کلاس ممیزی امنیت

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| **FAU\_GEN.1** | * FPT\_STM.1 |  | FAU\_GEN.1.1 | محصول باید براساس رخداد‌های قابل ممیزی زیر، رکورد ممیزی تولید نماید:   * آغاز و اتمام توابع ممیزی؛   تمامی رویداد‌های قابل ممیزی ( برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول 1 آمده است.  جدول1- لیست رویداد‌های قابل ممیزی   |  |  |  | | --- | --- | --- | | **جزئیات** | **رویداد قابل ممیزی** | **مولفه** | |  | تلاش­‌های ناموفق برای خواندن اطلاعات از رکورد‌های ممیزی (پایه) | مرتبط نمودن هویت کاربر به رویداد 1 | |  | خواندن اطلاعات از رکورد‌های ممیزی (پایه) | بازبینی داده ممیزی 1 | |  | ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌­افتد در حالی­که توابع ممیزی در حال انجام عملیات باشند. (حداقل) | انتخاب داده ممیزی 1 | |  | عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه) | اقدامات لازم در زمان از دست رفتن داده ممیزی 1 | |  | عملیات انجام شده به دلیل شکست ذخیره­سازی ممیزی (پایه) | پیشگیری از اتلاف و از بین رفتن داده­‌های ممیزی 1 | |  | تلاش­‌های موفقیت­آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل)  تمامی تلاش­ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه) | صحت داده‌های کاربری ذخیره شده 2 | |  | ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل)  ثبت تمام کاربرد‌های سازوکار احراز هویت (پایه) | احراز هویت کاربر | |  | ثبت نتایج احرازهویت (حداقل)  ثبت هر سازو کار احرازهویت فعال همراه با نتیجه نهائی (پایه) | سازوکار احرازهویت چندگانه | | شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال | تمامی کاربرد‌های سازوکارها برای شناسایی کاربر (موفق و ناموفق) | شناسایی کاربر | | برای مثال، رد و یا قبول کلمه عبور کاربر | ثبت رد هر کلمه عبور تست شده توسط محصول (حداقل)  ثبت تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول (پایه) | مدیریت کلمه عبور | |  | ثبت شکست انقیاد مشخصه­‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل)  شکست و موفقیت انقیاد مشخصه­‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه) | انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر | |  | تمامی تغییرات بر روی مقادیر مشخصه­‌های امنیتی (پایه) | مدیریت مشخصه­‌های امنیتی | | به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود. | تمامی تغییرات بر روی مقادیر داده­‌های امنیتی محصول (پایه) | مدیریت داده‌های محصول 1-مدیر سیستم | | به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود. | تمامی تغییرات بر روی مقادیر داده­‌های امنیتی محصول (پایه) | مدیریت داده‌های محصول 1-کاربرعادی، وارد کننده داده | |  | شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل)  هر حالتی از عملیات رمزنگاری کاربردی، مشخصه­‌های موجودیت­‌های فعال و غیر فعال (پایه) | عملیات رمزنگاری 1(1) | |  | شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل)  هر حالتی از عملیات رمزنگاری کاربردی، مشخصه­‌های موجودیت­‌های فعال و غیر فعال (پایه) | عملیات رمزنگاری 1 (2) | | شناسایی داده­‌های موجودیت غیرفعال | درخواست­‌های موفقیت­آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل)  تمامی درخواست­‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه) | عملیات کنترل دسترسی 1 | |  | ورود داده کاربری موفقیت آمیز، شامل هر گونه مشخصه­‌های امنیتی (حداقل)  تمامی تلاش­ها برای وارد کردن داده­‌های کاربری، شامل هر گونه مشخصه­‌های امنیتی (پایه) | ورود داده­‌های کاربری به محصول با مشخصه امنیتی | |  | خروج اطلاعات به­طور موفقیت­آمیز (حداقل)  همه تلاش­ها برای خارج کردن اطلاعات از محصول (پایه) | خروج داده‌های کاربری از محصول با مشخصه امنیتی | |  | تمامی تغییرات در رفتار‌های کارکردی محصول | مدیریت کارکرد در محصول | |  | ثبت استفاده از کارکرد‌های مدیریتی (حداقل) | کارکرد‌های مدیریتی محصول | |  | ثبت تغییرات در گروه­‌های کاربری که بخشی از یک نقش می‌­باشد (حداقل) | نقش­‌های امنیتی | |  | ثبت استفاده موفق از مکانیزم سازگاری داده­‌های محصول (حداقل)  ثبت استفاده از مکانیزم سازگاری داده­‌های محصول (پایه) | سازگاری داده­‌های امنیتی بین محصول و موجودیت امن | |  | ثبت شکست در محصول (پایه) | حفظ وضعیت امن در زمان شکست | |  | ثبت هر شکست شناسایی شده توسط محصول (حداقل)  ثبت تمامی قابلیت­‌های در حال قطع شدن محصول که به دلیل شکست می‌­باشد (پایه) | تحمل خطا | |  | ثبت منع آغاز نشست بدلیل مکانیزم آغاز نشست (حداقل)  ثبت تمامی تلاش­ها در آغاز نشست کاربر (پایه) | برقراری نشست 1 | |  | ثبت رد یک نشست مبتنی بر محدودیت نشست­‌های همزمان (حداقل) | محدودیت بر روی چندین نشست همزمان | |  | ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل)  ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل) | خاتمه دادن به نشست‌ها | |
|  | FAU\_GEN.1.2 | محصول باید برای هر ركورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:   * تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شكست) رویداد * ] **آدرس IP کاربر، نام و شناسه کاربری** [ |
| FAU\_GEN.2 | * FAU\_GEN.1 * FIA\_UID.1 |  | FAU\_GEN.2.1 | برای رویداد‌های ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید. |
| FAU\_SAR.1.1 | FAU \_ GEN.1 |  | FAU\_SAR.1.1 | محصول باید امکان خواندن/مشاهده ] **لیست کاربران، لیست سطوح دسترسی، تنظیمات سیستمی، سطوح دسترسی نقشه** [ از کل رکورد‌های ممیزی را برای ] **کاربر مدیر سیستم** [ فراهم نماید. |
| FAU\_SAR.1.2 |  | FAU\_SAR.1.2 | باید رکورد‌های ممیزی را طوری فراهم نماید که کاربر بتواند آن‌ها را درک و اطلاعات این رکورد‌ها را تفسیر نماید |
| FAU\_SAR.2.1 | FAU \_ SAR.1 |  | FAU\_SAR.2.1 | محصول باید مانع دسترسی خواندن رکورد‌های ممیزی توسط کلیه کاربران به غیر ازکاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند گردد. )الزام شماره 4) |
| FAU\_SAR.3.1 |  | FAU\_SAR.3.1 | محصول باید امکان انجام ] **متد‌های انتخاب و مرتب سازی** [ رکورد‌های ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس ] **حساب کاربری، تاریخ/زمان، نوع رخداد، و ] هیچ پارامتر دیگر[[** مرتب نماید. |
| FAU\_STG.1.1 | FAU\_ GEN.1 |  | FAU\_STG.1.1 | محصول باید رکورد‌های ممیزی ذخیره شده در محل ذخیره سازی را از حذف غیرمجاز حفاظت نماید. |
| FAU\_STG.1.2 |  | FAU\_STG.1.2 | محصول باید قادر به ] تشخیص، جلوگیری[ تغییرات غیرمجاز در رکورد‌های ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد. |
| FAU\_STG.3.1 | FAU \_ STG.1 |  | FAU\_STG.3.1 | محصول در صورت تجاوز دنباله ممیزی از ] **یک محدودیت از پیش تعریف شده** [ باید با استفاده **از ] یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسط‌های محصول کاربران مربوطه را [** مطلع نماید. |
| FAU\_STG. 4.1 |  | FAU\_STG. 4.1 | محصول در صورت پر شدن دنباله ممیزی، باید ] از ذخیره رویداد‌های قابل ممیزی، به جز آنهایی که توسط کاربر مجاز و تحت حقوق خاص رخ می‌‌دهند جلوگیری نماید [ و **]هیچ اقدام دیگری[** |
| FAU\_SEL.1.1 | FAU \_ GEN.1  FMT MTD.1 |  | FAU\_SEL.1.1 | محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخداد‌های قابل ممیزی شدن، انتخاب نماید:  ] هویت موجودیت فعال، نوع رخداد [  ] **هیچ معیار انتخاب دیگری** [ |

### کلاس پشتیبانی از رمزنگاری

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FCS\_COP.1.1(1) | [FDP \_ ITC.1,OR FDP \_ ITC.2,OR FCS \_ CKM.1]  FCS CKM. 4 |  | FCS\_COP.1.1(1) | محصول باید ] **برای وارسی صحت داده‌های ممیزی و داده‌های رکورد** [ بر اساس یک الگوریتم رمزنگاری مشخص ] **الگوریتم AES** [ و اندازه کلید ]**کلید 128 بیتی[** رمزنگاری اجرا شود که مطابق با ]  **استاندارد** [**FIPS PUB 197** باشد. |
| FCS\_COP.1.1(2) |  | FCS\_COP.1.1(2) | محصول باید ] **تولید داده درهمسازی [** بر اساس یک الگوریتم رمزنگاری مشخص ] **الگوریتم [SHA256**و اندازه کلید رمزنگاری ] **هیچ کدام** [ اجرا شود که مطابق با ] **SHA256**  [ باشد |
| FCS\_TLSC\_EXT.1.1 |  |  | FCS\_TLSC\_EXT.1.1 | محصول باید [TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌‌های رمز زیر را پیاده‌سازی نماید:  [   * TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA مطابق با RFC 3268 * TLS\_RSA\_WITH\_AES\_192\_CBC\_SHA مطابق با RFC 3268 * TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA مطابق با RFC 3268   [ |
| FCS\_TLSC\_EXT.1.2 |  |  | FCS\_TLSC\_EXT.1.2 | محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را از RFC 6125، تأیید نماید. |
| FCS\_TLSC\_EXT.1.3 |  |  | FCS\_TLSC\_EXT.1.3 | محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید ] ارتباط را برقرار نسازد، ]**هیچ اقدام دیگری**[[. |
| FCS\_TLSC\_EXT. 4.1 |  |  | FCS\_TLSC\_EXT. 4.1 | محصول باید در پیام Client Hello ] Supported Elliptic Curves Extension را ارائه نکند[ |
| FCS\_HTTPS\_EXT.1.1 |  |  | FCS\_HTTPS\_EXT.1.1 | محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند. |
| FCS\_HTTPS\_EXT.1.2 |  |  | FCS\_HTTPS\_EXT.1.2 | محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند. |
| FCS\_HTTPS\_EXT.1.3 |  |  | FCS\_HTTPS\_EXT.1.3 | درصورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [اتصال را برقرار ننماید]. |

### کلاس شناسایی و احرازهویت

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FIA\_PMG\_EXT.1.1 |  |  | FIA\_PMG\_EXT.1.1 | محصول باید قابلیت‌‌های مدیریت کلمه عبور را که در زیر ذکر شده‌اند برای کلمه‌‌های عبور مدیریتی فراهم نماید:  کلمه عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکتر‌های خاص: **]** ] "@"، "#"، "$"، "٪"، "^"، "!" "&"، "\*"، "(" , ")"] **هیچ کاراکتر دیگر**[[ باشد.  . حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و 8 کاراکتر یا بیشتر باشد. |
| FIA\_AFL.1.1 | FTA \_ UAU.1 |  | FIA\_AFL.1.1 | محصول، باید بتواند با استفاده [**3**]، یک عدد مثبت قابل تنظیم توسط مدیر**]بین 3 الی 5[** تلاش ناموفق احراز هویت مرتبط با ] **احراز هویت کاربر در هنگام ورود به سامانه** ، **اعتبار‌سنجی پسورد قدیم در هنگام تغییر پسورد** [ را تشخیص دهد. |
| FIA\_UID.1.1 |  |  | FIA\_UID.1.1 | محصول باید پیش از شناسایی کاربر اجازه اقدامات زیر را فراهم آورد:  ]   * مشاوره راهنمای نحوه ورود به سیستم، * دانلود افزونه‌های کمکی * هیچ اقدام دیگری   [ |
| FIA\_UID.1.2 |  |  | FIA\_UID.1.2 | توابع امنیتی هدف ارزیابی، باید هر كاربر را پیش از آنكه امكان انجام اقدامات می‌انی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی نماید. |
| FIA\_AFL.1.2 | FTA \_ UAU.1 |  | FIA\_AFL.1.2 | زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت ] به حد تعیین شده رسید و یا از آن بیشتر شد [، محصول باید ]**کاربر را به مدت تعیین شده قفل نماید** [ را اجرا نماید که باعث پیچیدهتر کردن عمل احراز هویت مجدد کاربر شود. |
| FIA\_ATD.1.1 |  |  | FIA\_ATD.1.1 | محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید:  ]  **شناسه کاربر**  **متد احرازهویت مورد استفاده**  **داده‌های احراز هویت**  **نقش کاربر**  **وضعیت حساب کاربری )فعال، غیرفعال، بلوکه شده و غیره(**  ]**هیچ مشخصه امنیتی دیگر** [  [ |
| FIA\_UAU.1.1 | FTA \_ UID.1 |  | FIA\_UAU.1.1 | محصول باید پیش از احرازهویت کاربر، اجازه اقدامات می‌انی زیر را به کاربر دهد:  ]   * مشاهده راهنمای نحوه ورود به سیستم * شناسایی کاربر * بازیابی کلمه‌عبور * هیچ اقدامی * ] **هیچ اقدامات دیگری**[   [ |
| FIA\_UAU.1.2 |  | FIA\_UAU.1.2 | محصول باید هر كاربر را پیش از آنكه امكان انجام اقدامات می‌انی دیگری داشته باشد، با موفقیت احرازهویت نماید. |
| FIA\_UAU. 5.1 |  |  | FIA\_UAU. 5.1 | محصول باید به منظور احرازهویت کاربر سازوکار‌های زیر را فراهم آورد:  ]   * نام کاربری و کلمه عبور * احراز هویت دو مرحله با استفاده از شماره موبایل یا پست الکترونیک   [. |
| FIA\_UAU. 5.2 |  |  | FIA\_UAU. 5.2 | محصول باید هر کاربر متقاضی احرازهویت را مطابق قوانین ذیل احرازهویت نماید:  ]   * کاربران از راه‌دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احرازهویت چندگانه (مانند Dual factor authentication) استفاده کند. * احراز هویت دو مرحله با استفاده از شماره موبایل یا پست الکترونیک   [ |
| FIA\_USB.1.1 | FTA \_ ATD.1 |  | FIA\_USB.1.1 | محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:  ]  **شناسه کاربر**  **نقش‌های کاربر**  **جزئیات واسط کلاینت**  **پیشینه احرازهویت )زمان آخرین تلاش احرازهویت موفق و ناموفق(**  ] **هیچ مشخصه‌ی کاربری دیگر** [  [ |
| FIA\_USB.1.2 |  | FIA\_USB.1.2 | محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:  ]   * زمانی­که یک نشست جدید برقرار می‌­شود، اعتبار نشست­‌های قبلی باید از بین برود (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد و هنگام فعال شدن نشست دوم و بیشتر در برنامه، باید به صفحه کاربر نشست اصلی(اول) اطلاع داده شود. ) * اطلاعات پیشینه احراز هویت باید بروزرسانی گردد.   ] **هیچ قوانین دیگر** [  [ |
| FIA\_USB.1.3 |  | FIA\_USB.1.3 | محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید:  ]**هیچ تغییری در طول نشست فعال مجاز نمی باشد**[،  ]**هیچ قوانین دیگر** [ |
| FIA\_X509\_EXT.1.1 |  |  | FIA\_X509\_EXT.1.1 | محصول مورد ارزیابی 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 مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌‌های CA به حالت «True» تنظیم‌شده است * محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [هیچ روش فسخ] تأیید کند. * محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند: * گواهی‌نامه‌‌های مورداستفاده برای تأیید 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. |
| FIA\_X509\_EXT.1.2 |  |  | FIA\_X509\_EXT.1.2 | محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌‌پذیرد. |
| FIA\_X509\_EXT.1.3 |  |  | FIA\_X509\_EXT.1.3 | محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای [HTTPS]، و [امضای کد برای به‌روزرسانی‌‌های نرم‌افزار سیستم [**هیچ کاربرد دیگر**] از گواهی‌نامه‌‌های X. 509v3 تعریف‌شده در RFC 5280 استفاده کند. |
| FIA\_X509\_EXT.2.2 |  |  | FIA\_X509\_EXT.2.2 | در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید ]گواهی را نپذیرد. [ |

### کلاس حفاظت از داده کاربری

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FDP\_RIP.2.1 | [FDP \_ ACC.1,OR FDP \_ IFC.1]  [FTP \_ ITC.1,OR FTP \_ TRP.1]  FPT \_ TDC.1 |  | FDP\_RIP.2.1 | محصول باید تضمین نماید در هنگام ] تخصیص منابع به، آزادسازی منابع از[ تمام موجودیت­‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می‌­گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد. |
| FDP\_ITC.2.1 |  | FDP\_ITC.2.1 | محصول باید هنگام دریافت داده کاربری، ] **خطمشی کنترل دسترسی [** را اعمال نماید. |
| FDP\_ITC.2.2 |  | FDP\_ITC.2.2 | محصول باید از مشخصه‌های امنیتی مرتبط با داده کاربری هنگام وارد کردن داده استفاده نماید. مشخصات امنیتی شامل مواردی از این قبیل است:  نوع داده، حجم و اندازه فایل، فرمت فایل، تعداد دفعات Import و از این قبیل موارد. |
| FDP\_ITC.2.3 |  | FDP\_ITC.2.3 | محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه­‌های امنیتی و داده کاربری دریافت شده، فراهم می‌­نماید. |
| FDP\_ITC.2. 4 |  | FDP\_ITC.2. 4 | محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، می‌باشد. |
| FDP\_ITC.2. 5 |  | FDP\_ITC.2. 5 | محصول باید هنگام ورود داده کاربری از بیرون )خارج از محصول(، قوانین تحت کنترل خطمشی امنیتی زیر را اعمال نماید:  ] **هیج قوانین دیگر**. [ |
| FDP\_SDI.2.1 |  |  | FDP\_SDI.2.1 | محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص ] **خطا‌های صحت داده**[ داده­‌های رکورد و داده­‌های ممیزی را بر اساس مشخصه­‌های ] **درهم شده[[2]](#footnote-2) داده­‌های کاربری ذخیره شده**[ پایش نماید |
| FDP\_SDI.2.2 |  |  | FDP\_SDI.2.2 | هنگام تشخیص خطای صحت داده، محصول باید ] **اطلاع به کاربر و ممانعت از ثبت داده** [ را صورت دهد. |
| FDP\_ACC.1.1 | FDP \_ ACF.1 |  | FDP\_ACC.1.1 | محصول باید ] **خطمشی‌های کنترل دسترسی** [ را بر روی موارد زیر اعمال نماید:  ]  **موجودیت فعال** ] **مدیر سیستم، کاربر عادی، ] هیچ موجودیت فعال دیگری[**  **موجودیت غیرفعال:**   * **رکوردها، مستندات** * **داده‌های متعلق به کاربر** * **داده احرازهویت** * **داده با این معیارها ] هیچ معیار داده دیگر[** * ] **هیچ موجودیت‌های غیر فعال دیگری** [   **ایجاد موجودیت غیرفعال جدید**   * **حذف موجودیت غیرفعال** * **تغییر دسترسیها به موجودیت غیرفعال** * **عملیات بر روی فرداده‌های وابسته به موجودیت غیرفعال** * **] هیچ عملیات دیگری** [   [ |
| FDP\_ACF.1.1 | FDP \_ ACC.1  FMT\_ MSA.3 |  | FDP\_ACF.1.1 | محصول باید ]**خط­مشی­‌های کنترل دسترسی[** را با توجه به موارد زیر بر روی موجودیت­‌های غیرفعال اعمال نماید:  ]   * **هویت کاربر** * **نقش­ها و مجوز‌های کاربر مجاز** * **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌­شوند** * **]هیچ مشخصه دیگری[**   **[** |
| FDP\_ACF.1.2 |  | FDP\_ACF.1.2 | محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید:  ] **عملیات تنها به شرطی مجاز است 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.** [ |
| FDP\_ACF.1.3 |  | FDP\_ACF.1.3 | محصول باید براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد:  **کاربران با مجوز مدیر سیستم به رکورد­‌های لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند.**   * **کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.** * **] هیچ قانون دیگری** [   [ |
| FDP\_ACF.1. 4 |  | FDP\_ACF.1. 4 | محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری ­نماید:  ] تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[[3]](#footnote-3) از پیش تعریف شده،  ] **هیچ قانون دیگری** [ [. |

### کلاس مدیریت امنیت

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FMT\_MOF.1.1 | FMT \_ SMR.1  FMT \_ SMF.1 |  | FMT\_MOF.1.1 | محصول باید امکان ] تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار[ توابع ]**تمام کارکرد‌های مربوط به مدیریت محصول**[ را به ]ا **مدیر سیستم و هر کاربری که مجوز لازم را دارد،** ] **هیچ نقش دیگیری**[[ محدود نماید. |
| FMT\_MSA.1.1 | [FDP \_ ACC.1OR FDP \_ IFC.1]  FMT \_ SMR.1  FMT \_ SMF.1 |  | FMT\_MSA.1.1 | محصول باید با اعمال ] خط­مشی کنترل دسترسی[،]امکان تغییر پیش‌فرض، پرس و جو، تغییر، حذف، ]هیچ عملیات دیگر [[ مشخصه­‌های امنیتی  ]   * شناسه کاربر * نقش­ها و یا مجموعه دسترسی­‌های کاربر به قسمت‌های مختلف برنامه * جزئیات واسط کلاینت * پیشینه احرازهویت (جزیئات تلاش برای احرازهویت موفق و ناموفق) * ]هیچ مشخصه کاربری دیگر[   [ را به ] مدیر سیستم و هر کاربری که مجوز لازم را دارد [ محدود نماید |
| FMT\_MSA.3.1 | FMT \_ MSA.1  FMT \_ SMR.1 |  | FMT\_MSA.3.1 | محصول برای مشخصه‌های امنیتی که برای اعمال ] **خط مشی** [ استفاده می‌شوند، باید مقادیر پیش فرض محدود شد‌های درنظر بگیرد. |
| FMT\_MSA.3.2 |  | FMT\_MSA.3.2 | محصول برای تعیین مقادیر اولیه پیشنهادی باید به ] **مدیر سیستم** [ اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیشفرض را لغو و تغییر دهد. |
| FMT\_MTD.1.1(1) | FMT \_ SMR.1  FMT \_ SMF.1 |  | FMT\_MTD.1.1(1) | محصول باید توانایی ] تغییر پیشفرض، پرسوجو، تغییر، حذف، پاک نمودن، **]هیچ کارکرد دیگری** ] [**رویداد‌‌های ممیزی، داده‌‌های احراز هویت و تنظیمات امنیتی [** به ] **مدیر سیستم،** ] **هیچ نقش دیگری** [ [ محدود نماید. |
| FMT\_MTD.1.1(2) |  | FMT\_MTD.1.1(2) | محصول باید امکان ] تغییر پیش‌فرض، پرس­و­جو، تغییر، حذف، پاک نمودن، ] **هیچ کارکرد دیگری**[ [ ] **پسورد کاربر، شماره‌ی تماس و یا آدرس ایمیل (که برای مقاصد امنیتی نظیر بازیابی رمز عبور و یا ارسال رمز یکبار مصرف** [ را به ] **مدیر سیستم و هر کاربری که مجوز لازم را دارد**[ محدود نماید |
| FMT\_SMF.1.1 |  |  | FMT\_SMF.1.1 | محصول باید قادر به انجام ] **کارکرد‌های مدیریتی که در جدول زیر آمده است [** باشد.   | **مولفه** | **عملیات مدیریتی** | | --- | --- | | بازبینی داده ممیزی 1 | پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکورد‌های ممیزی | | انتخاب داده ممیزی 1 | پشتیبانی از مجوز‌های مشاهده/ویرایش رویداد‌های ممیزی | | اقدامات لازم در زمان از دست رفتن داده ممیزی 1 | پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره­سازی ممیزی | | پیشگیری از اتلاف و از بین رفتن داده­‌های ممیزی 1 | پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره­سازی ممیزی | | عملیات کنترل دسترسی | مدیریت مشخصه­‌های مورد استفاده برای ایجاد دسترسی و یا منع | | حفاظت کامل از اطلاعات باقیمانده در منابع | انتخاب هنگام اجرای حفاظت از اطلاعات باقی­مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌­تواند در محصول قابل پیکربندی باشد. | | ورود داده‌های کاربری به محصول با مشخصه امنیتی | ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول | | صحت داده‌های کاربری ذخیره شده 2 | عملیاتی برای تشخیص یک خطای صحت داده که می‌­تواند قابل پیکربندی باشد. | | مدیریت احراز هویت ناموفق | مدیریت حدآستانه برای تلاش­‌های ناموفق  مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد. | | تعریف مشخصات کاربر | مدیر مجاز باید قادر به تعریف مشخصه­‌های امنیتی بیشتر برای کاربران باشد. ]اختیاری[ | | مدیریت کلمه عبور | مدیریت تنظیمات و الزامات و قابلیت­ها برای تنظیم کلمه عبورها | | احراز هویت کاربر | مدیریت داده­‌های احرازهویت توسط مدیر یا کاربر مرتبط  مدیریت یکسری عملیاتی که قبل از احرازهویت کاربر انجام می‌­شوند. | | سازوکار احرازهویت چندگانه | مدیریت سازوکار‌های احرازهویت  مدیریت قوانین مرتبط با احرازهویت | | شناسایی کاربر | مدیریت شناسایی کاربران]اختیاری[  مدیریت تغییرات و فرایندهایی مانند(اختصاص ادرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌­تواند قبل از شناسایی کاربر انجام دهد. | | انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر | مدیر مجاز می‌­تواند مشخصه­‌های امنیتی موجودیت­‌های فعال پیش­فرض را تعریف و تغییر دهد. | | مدیریت مشخصه­‌های امنیتی | مدیریت گروهی از نقش­هایی که با مشخصه­‌های امنیتی در تعامل هستند. | | مقدار دهی اولیه مشخصه­ها | مدیریت گروهی از نقش­هایی که مقادیر اولیه را مشخص می‌­کنند.  مدیریت مقادیر پیش­فرض برای کنترل دسترسی محصول | | مدیریت داده‌های محصول 1-مدیر سیستم | مدیریت گروهی از قوانینی مرتبط با داده­‌های محصول | | مدیریت داده‌های محصول 1-کاربرعادی، وارد کننده داده | مدیریت گروهی از قوانینی مرتبط با داده­‌های محصول | | نقش­‌های امنیتی | مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند. | | محدودیت بر روی چندین نشست همزمان | مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر | | برقراری نشست | مدیریت شرایط آغاز نشست توسط مدیر مجاز | | خاتمه دادن به نشست‌ها | تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد.  تعیین زمان پیش­فرض غیرفعال بودن کاربر که نشست خاتمه یابد. | |
| FMT\_SMR.1.1 | FTA \_ UID.1 |  | FMT\_SMR.1.1 | نقش‌های زیر در محصول باید تعریف شده باشد:  ] مدیر سیستم،کاربر عادی،] **هیچ نقش دیگر** [[ |
| FMT\_SMR.1.2 |  | FMT\_SMR.1.2 | محصول، باید قادر به مرتبط نمودن كاربران با نقش‌ها و دسترسی­‌های مجاز تعریف شده باشند. |

### کلاس حفاظت از توابع امنیتی هدف ارزیابی

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FPT\_FLS.1.1 |  |  | FPT\_FLS.1.1 | محصول باید در زمان رخداد انواع شکست­‌های زیر، وضعیت امن را حفظ نمایند:  ] **شکست­‌های نرم­افزاری، شکست­‌های سخت‌افزاری** [ |
| FPT\_TDC.1.1 |  |  | FPT\_TDC.1.1 | محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار ] **نام کاربری،شماره موبایل،کلمه عبور،اطلاعات سطوح دسترسی،توکن اتصال امن**[ را در زمان اشتراک گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. |
| FPT\_TDC.1.2 |  |  | FPT\_TDC.1.2 | محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، ]   * **API‌های ارایه شده برقراری ارتباط با وب‌سرویس‌ها** * **API مربوط به ارسال پیامک ورود دو عامله**   [ استفاده نماید. |
| FPT\_ITT.1.1 |  |  | FPT\_ITT.1.1 | محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده­ در هنگام انتقال بین بخش­‌های مجزای خود که باهم ارتباط دارند، محافظت نماید. |
| FPT\_STM.1.1 | افتا |  | FPT\_STM.1.1 | توابع امنیتی هدف ارزیابی باید قادر به ایجاد مهر‌های زمانی قابل اطمینان باشند. |
| 2(FPT\_TUD\_EXT.1.2) | افتا |  | 2(FPT\_TUD\_EXT.1.2) | محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولید کننده محصول فراهم نماید که به‌روزرسانی نرم‌افزار و می‌ان‌افزارمحصول مورد ارزیابی را به صورت دستی آغاز نماید و [از هیچ مکانیسم به‌روزرسانی پشتیبانی نکند]. |

### کلاس دسترسی به هدف ارزیابی

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FTA\_MCS.1.1 | FTA \_ UID.1 |  | FTA\_MCS.1.1 | محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید. |
| FTA\_MCS.1.2 |  | FTA\_MCS.1.2 | محصول باید به صورت پیشفرض، ] **5 [** برای هر کاربر در نظر بگیرد. |
| FTA\_SSL.3.1 |  |  | FTA\_SSL.3.1 | محصول باید کلیه نشست­‌های تعاملی راه‌دور را پس از مدت زمان ] **دو ساعت**[ غیرفعال بودن، خاتمه دهد. |
| FTA\_SSL. 4.1 |  |  | FTA\_SSL. 4.1 | محصول باید به کاربری که خود آغازگر نشست بوده است اجازه­ی خاتمه نشست را بدهد. |
| FTA\_TAH.1.2 |  |  | FTA\_TAH.1.2 | در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید ] زمان [ آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش‌های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد. |
| FTA\_TAH.1.3 |  |  | FTA\_TAH.1.3 | توابع امنیتی هدف ارزیابی نباید اطلاعات تاریخچه دسترسی را از واسط کاربری پاک نماید، بدون اینکه به کاربر فرصتی داده شود تا اطلاعات را بازبینی نماید. |
| FTA\_TSE.1.1 |  |  | FTA\_TSE.1.1 | توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس] **مکان، شماره پورت، تعداد تلاش‌های ناموفق احرازهویت، شناسه کاربر( نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP** ] ]**بدون مشخصه دیگر**[ممانعت نماید. |
| FTA\_TAH.1.1 |  |  | FTA\_TAH.1.1 | در صورت برقراری نشست به طور موفقیت­آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست براساس ] زمان، ] **هیچ مشخصه دیگری**[[ باشد. |

### كلاس كانال‌ها و مسیر‌‌های مورد اعتماد

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FTP\_ITC.1.1 | افتا |  | FTP\_ITC.1.1 | محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [HTTPS,TLS] می‌ان خود و موجودیت IT معتبر، [سرور ممیزی، سرور احرازهویت، ]**هیچ قابلیت دیگری**]] که به طور منطقی از کانال­‌های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده‌‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. |
| FTP\_ITC.1.2 |  | FTP\_ITC.1.2 | محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند. |
| FTP\_ITC.1.3 |  | FTP\_ITC.1.3 | محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای  [   * **ارسال پیامک (ایمیل) جهت ارسال رمز عبور یک‌بار مصرف به کاربران** * **ارسال ایمیل جهت بازیابی پسورد کاربران**   ]  راه‌اندازی نماید. |
| FTP\_TRP.1.1 | افتا |  | FTP\_TRP.1.1 | محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [HTTPS] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال­ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده­‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد. |
| FTP\_TRP.1.2 |  | FTP\_TRP.1.2 | محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند. |
| FTP\_TRP.1.3 |  | FTP\_TRP.1.3 | محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی کند. |

### كلاس تخصیص منابع

| مؤلفه | وابستگی ها | شماره | المان | شرح المان |
| --- | --- | --- | --- | --- |
| FRU\_FLT.1.1 | FPT \_ FLS.1 |  | FRU\_FLT.1.1 | محصول باید از عملکرد ] **تمام کارکرد‌های اصلی** [ هنگام رویداد شکست­‌های زیر اطمینان حاصل نماید:  ] **شکست نرم­افزاری**، ] **هیچ شکست دیگری**[[ |

## توجیهات

|  |  |
| --- | --- |
| **نام الزام** | **شرح عدم پیاده سازی** |
| **FPT\_TUD\_EXT.1.3** | محصول به روزرسانی خودکار ندارد. |
| **FDP\_ETC.2** | در خروج داده کاربری از محصول، از هیچ گونه مشخصه‌ی امنیتی مانند امضاء دیجیتال استفاده نشده است. |

## الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 بر اساس الزامات بخش سوم استاندارد ISO/IEC15408 آورده می‌­شود که لیست الزامات آن در جدول زیر آمده است.

|  |  |  |
| --- | --- | --- |
| **نام کلاس** | **نام مؤلفه** | **توضیحات** |
| **Development** | ADV\_FSP.1 | مشخصات کارکرد ابتدایی |
| **Guidance Documents** | AGD\_OPE.1 | راهنمای کاربری |
| AGD\_PRE.1 | راهنمای آماده­سازی |
| **Security Target** | ASE\_CCL.1 | ادعا‌های انطباق |
| ASE\_ECD.1 | تعریف مؤلفه‌‌های توسعه‌یافته |
| ASE\_INT.1 | معرفی هدف امنیتی |
| ASE\_OBJ.1 | اهداف امنیتی |
| ASE\_REQ.1 | الزامات امنیتی معین |
| ASE\_TSS.1 | خلاصه مشخصات هدف ارزیابی |
| **Tests** | ATE\_IND.1 | آزمون مستقل-منطبق |
| **Vulnerability Assessment** | AVA\_VAN.1 | تحلیل آسیب­پذیری |
| **Life cycle Support** | ALC\_CMC.1 | برچسب گذاری هدف ارزیابی |
| ALC\_CMS.1 | پوشش پیکربندی هدف ارزیابی |

# خلاصه مشخصات هدف ارزیابی

هدف این قسمت ارائه دادن شرحی از چگونه برآورده نمودن تمام الزامات کارکرد امنیتی توسط هدف ارزیابی به مصرف کنندگان می‌­باشد.

**تولید داده ممیزی**

* روش فراخوانی: بوسیله کنش‌های هر کاربر قبل و/یا هنگام و/یا بعد از هر عمل در سامانه.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست.
  + نام کاربر: نام و شهرت کاربر که در سامانه ثبت است.
  + نوع عمل: نوع کلی عمل مانند مشاهده، ویرایش، ایجاد، بارگیری و ...
  + نام بخش: بخشی از سامانه که کاربر عمل خود را صورت‌داده مانند بخش مدیریت کاربران.
  + شرح عملیات: شرح دقیق عملی که رخ‌داده با جزئی‌ترین اطلاعات.
  + تاریخ و ساعت: تاریخ و زمان عملی که کاربر انجام‌داده‌است.
  + نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده
  + نتیجه: ثبت موفق رویداد

**بازبینی داده‌های ممیزی**

* روش فراخوانی: کاربر مجاز ازطرق زیر دسترسی به داده‌های ممیزی دارد:
  + منو > رویدادهای ممیزی > لاگین‌های کاربران
  + منو > امکانات > گزارش کاربران سیستم
  + منو > امکانات > بررسی پیام‌های سیستم
  + منو > امکانات > بررسی پیام‌های IIS
* پارامترهای قابل تنظیم:
  + ‌شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: عدم امکان خواندن اطلاعات ممیزی برای کاربران غیرمجاز

**انتخاب داده‌های ممیزی**

* روش فراخوانی: کاربر مجاز (دارای دسترسی "تعاریف > فیلتر رویدادهای ممیزی" می‌تواند بین مواردی که در مسیر "تعاریف > فیلتر رویدادهای ممیزی" وجود دارد، انتخاب نماید که کدام رویداد ممیزی ثبت شود.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای بررسی دسترسی‌های کاربر
  + الزام ثبت رویدادهای فعالیت کاربران: درصورت انتخاب شدن رویدادهای فعالیت کاربران ثبت می‌شوند.
  + الزام ثبت رویدادهای ورود/خروج کاربران: درصورت انتخاب شدن رویدادهای ورود/خروج کاربران ثبت می‌شوند.
  + الزام ثبت رویدادهای پیام‌های سیستم: درصورت انتخاب شدن رویدادهای پیام‌های سیستم ثبت می‌شوند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: نمایش خطا درصورت عدم دسترسی کاربر به بخش مذکور
  + نتیجه موفق: ویرایش سیاست‌های فیلتر رویدادهای ممیزی

**ذخیره رویدادهای ممیزی**

* روش فراخوانی: بوسیله کنش‌های هر کاربر قبل و/یا هنگام و/یا بعد از هر عمل در سامانه.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر.
  + رکورد ممیزی: بمنظور بازدرهم‌سازی رکورد که درنهایت این مقدار درهم جدید با مقدار درهم موجود در پایگاه‌داده سنجیده‌شده و نتیجه این سنجش به کاربر نمایش‌داده‌می‌شود.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: سنجش اعتبارسنجی به کاربر نمایش‌داده می‌شود.
  + نتیجه ناموفق: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده
  + پیام خطا: درصورت عدم دسترسی کاربر به بخش مذکور

**ازبین‌رفتن داده‌های ممیزی**

* روش فراخوانی: درصورت تجاوز دنباله‌ی ممیزی از حد آستانه هشدار ویا از حد آستانه بحران.
* پارامترهای قابل تنظیم:
  + شماره تماس کاربر: شماره تماسی که برای فرستادن پیامک اطلاع‌رسانی استفاده می‌شود.
  + نام جدول ممیزی پُرشده: جدول ممیزی پرشده که قصد خالی‌سازی فضای آنرا داریم.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه ناموفق: درصورت ثبت‌نبودن شماره تماس کاربر مربوطه، یک رکورد ممیزی با همین مضمون ثبت می‌گردد.
  + نتیجه ناموفق: درصورت عدم توانایی فرستادن اعلان پیامکی، یک رکورد ممیزی با همین مضمون ثبت می‌گردد.
  + نتیجه موفق: درصورت موفق‌آمیز بودن، فضای خالی برای ثبت رکوردهای ممیزی جدید فراهم می‌گردد.

**عملیات رمزنگاری**

* روش فراخوانی:
  + هنگام استفاده از الگوریتم رمزنگاری برای صحت‌سنجی داده‌های احراز هویت، داده‌های ممیزی و داده‌های رکورد
  + هنگام استفاده از الگوریتم رمزنگاری برای تولید داده‌های درهم‌شده (Hash)
* پارامترهای قابل تنظیم:
  + نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند.
  + متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: یک مقدار درهم‌شده خواهد بود.

**خط‌مشی و عملیات مهار دسترسی**

* روش فراخوانی: به‌ازای هر کنش کاربر در سامانه، دسترسی‌های او به موجودیت‌های فعال ویا غیرفعال درخواستی کنترل و مهار می‌شود. کاربر مجاز سطح مدیر توانایی افزودن یا کاستن دسترسی‌های کاربران دیگر را ازطرق زیر دارا هستند:
  + منو > مدیریت کاربران > سطح دسترسی
  + منو > مدیریت کاربران > دسترسی و گروه‌بندی کاربران
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای شناسایی اینکه آیا کاربر به بخش درخواستی خود دسترسی دارد یا خیر استفاده می‌شود.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورتی که کاربر به بخش درخواستی خود دسترسی نداشته باشد.
  + نتیجه موفق: درصورتی که کاربر بخش مذکور دسترسی داشته باشد، عملیات صورت می‌گیرد.
  + نتیجه: در هر دو حالت قبل یک رویداد ممیزی مرتبط ثبت می‌شود.
  + نتیجه: درصورتی تجاوز از حد آستانه تعداد نشست‌های هم‌زمان، پیامکی ارسال می‌شود.

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

* روش فراخوانی: کاربر می‌تواند به مسیر زیر رفته و پس‌از انتخاب شماره پرونده اقدام به بارگذاری داده کند: منو > آرشیو > آرشیو الکترونیک > آپلود

درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد.ب ایست خاطرنشان کرد که سامانه فعلی از سازوکار امضای دیجیتال پشتیبانی نمی‌کند.

* پارامترهای قابل تنظیم:
  + شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد.
  + داده بارگذاری‌شده: هر آنچه که کاربر قصد بارگذاری آن را دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: درصورت موفقت‌آمیز بودن، داده کاربر در سرور ذخیره می‌شود.
  + پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر.
  + نتیجه: در هر دو حالت قبل رویداد ممیزی ثبت می‌گردد.

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

* روش فراخوانی: ‌کاربر می‌تواند درصورت داشتن دسترسی بارگیری در بخش‌های دارای این دسترسی (مثلا دکمه‌هایی با متن "خروجی اکسل")، اقدام به بارگیری (download) کند. درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد.
  + داده قابل‌بارگیری: هر آنچه که کاربر قصد بارگیری آن را دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر.
  + نتیجه: رویداد ممیزی مرتبط شامل اطلاعات حائز امنیت ثبت می‌گردد.

**صحت داده کاربری ذخیره‌شده**

* روش فراخوانی: کاربر مجاز با مراجعه به بخش‌های زیر می‌تواند از معتبر بودن یا نبودن داده‌‌ مطلع گردد:
  + منو > رویدادهای ممیزی > لاگین‌های کاربران
  + منو > امکانات > گزارش کاربران سیستم
  + منو > امکانات > بررسی پیام‌های سیستم
  + منو > امکانات > بررسی پیام‌های IIS
* پارامترهای قابل تنظیم:
  + نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند.
  + متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: نتیجه یکی از دو حالت "معتبر" یا "نامعتبر" است که به کاربر نمایش‌داده‌می‌شود.

**مدیریت احراز هویت ناموفق**

* روش فراخوانی: کاربری که نشست فعال نداشته‌باشد، هنگام واردکردن اطلاعات احراز هویت خود در صفحه ورود به سامانه دچار خطا شود و نتواند به سامانه ورود پیدا‌کند. درصورت تکرار این خطا، رویه ورود پیچیده‌تر شده و از کد کپچا استفاده می‌گردد. همچنین کاربر مدیر سیستم می‌تواند با تعیین مدت جریمه زمانی، کاربری که تلاش ناموفق فراوان داشته است را تا مدت زمان مشخصی مسدود نماید. کاربر در این مدت زمان حتی با واردکردن اطلاعات هویتی صحیح نیز قادر به ورود به سامانه نخواهد بود. پس از این مدت زمان همه چیز به روال عادی خود برمی‌گردد و کاربر درصورت واردکردن اطلاعات هویتی صحیح می‌تواند وارد سامانه گردد. علاوه‌براین سامانه‌ی فعلی از سازوکار ارتباط از راه‌دور ازطریق SSH پشتیبانی نمی‌کند.
* پارامترهای قابل تنظیم:
  + حد آستانه تلاش ناموفق ورود: عددی مثبت که کاربر سطح مدیر وارد سامانه می‌کند.
  + کد کپچا: یک عبارت تصادفی که برای پیچیده‌سازی فرآیند ورود بکار می‌رود.
  + جریمه زمانی: مدت زمانی که در آن کاربری که تلاش ناموفق فراوان داشته، نمی‌تواند به سامانه وارد شود. این مقدار توسط کاربر مدیر سیستم (سطح بالا) قابل تنظیم است.
  + داده‌های احراز هویت کاربر: نام کاربری و رمزعبوری که کاربر برای ورود استفاده می‌کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت تجاوز از حد آستانه، پیام مرتبط به کاربر نمایش‌داده‌می‌شود.
  + نتیجه ناموفق: درصورت تجاوز از حد آستانه، کد کپچا فعال می‌شود.

**تعریف مشخصات کاربر**

* روش فراخوانی: بمحض ورود موفق کاربر به سامانه و ایجاد نشست فعال، فراخوانی می‌شود. و داده‌های زیر از کاربر فعال ذخیره می‌شود:
  + شناسه کاربر
  + متد احراز هویت مورد استفاده
  + داده احراز هویت
  + وضعیت حساب کاربری

همچنین کاربر با مراجعه به منوی بالا سمت چپ سامانه و با فشردن دکمه "تغییر رمز عبور" می‌تواند اقدام به تغییر رمز عبور خود کند.

* پارامترهای قابل تنظیم:
  + شناسه کاربر: نام کاربری که در سامانه تعریف‌شده‌باشد.
  + متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ...
  + داده احراز هویت: شامل نام کاربری و رمزعبور کاربر.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + ‌نتیجه موفق: داده‌ها و مشخصه‌های امنیتی کاربر ذخیره می‌شوند.

**مدیریت کلمه عبور**

* روش فراخوانی: ‌کاربر سطح مدیر می‌تواند تمامی این سیاست‌ها را در مسیر "تعاریف > پنل کاربری > تنظیمات پسورد" تعیین کند.
* پارامترهای قابل تنظیم:
  + شامل عدد بودن: الزامی بودن وجود ارقام در کلمه عبور را مشخص می‌کند.
  + شامل حروف بودن: الزامی بودن وجود حروف در کلمه عبور را مشخص می‌کند.
  + شامل علائم بودن: الزامی بودن وجود نویسه‌های خاص در کلمه عبور را مشخص می‌کند. مانند: ~×!@#$%^&\*()
  + طول پسورد: حداقل طول کلمه عبور را مشخص می‌کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌شوند.
  + نتیجه: رویداد ممیزی ثبت می‌شود.
  + پیام خطا: بدلیل عدم دسترسی کاربر به بخش موردنظر.

**احراز هویت کاربر**

* روش فراخوانی: در صفحه ورود کاربران (LOGIN) کاربر می‌تواند اقدامات میانی زیر را بدون نیاز به احراز هویت انجام دهد:
  + بازیابی رمزعبور
  + شناسایی کاربر

باقی موارد و امکانات سامانه نیازمند به احراز هویت موفق کاربر هستند. کاربری می‌تواند احراز هویت کند که از قبل هیچ نشست فعالی نداشته‌باشد. در شرایطی که احراز هویت دو مرحله ای فعال باشد، کاربر باید اقدام به دریافت رمز یکبار مصرف از طریق پیامک و واردکردن آن در فیلد مربوطه نماید.

* پارامترهای قابل تنظیم:
  + داده احراز هویت: نام کاربری و رمزعبور کاربر بمنظور ورود موفق به سامانه
  + شماره تماس کاربر: بمنظور بازیابی رمزعبور
  + کد تایید دومرحله‌ای: درصورتی که این تنظیمات فعال باشد، کاربر بایست کد تاییدی که دریافت کرده است را وارد سامانه نماید.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت عدم انطباق شماره تماس کاربر با اطلاعات ذخیره‌شده در سامانه
  + پیام خطا: درصورت ورود ناموفق کاربر
  + نتیجه موفق: ورود موفق درصورت تصدیق داده‌های هویتی کاربر

**سازوکار احراز هویت چندگانه**

* روش فراخوانی: در صفحه ورود کاربران (LOGIN) کاربری می‌تواند احراز هویت کند که از قبل هیچ نشست فعالی نداشته‌باشد. در شرایطی که احراز هویت دو مرحله ای فعال باشد، کاربر باید اقدام به دریافت رمز یکبار مصرف از طریق پیامک و واردکردن آن در فیلد مربوطه نماید.

کاربر می‌تواند از طرق مختلف احراز هویت صورت‌دهد. مانند:

* + نام کاربری و رمزعبور
  + تایید دومرحله‌ای
  + استفاده از رمز یکبارمصرف
* پارامترهای قابل تنظیم:
  + نام کاربری و رمزعبور: اطلاعاتی که کاربر برای ورود نیاز دارد.
  + شماره تماس: بمنظور ارسال کد تایید در سازوکار ورود با شماره تماس
  + کد تایید دومرحله‌ای: یک دنباله تصادفی برای تایید گام دوم ورود کاربر
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت اشتباه‌بودن کد تایید، نام کاربری و رمزعبور.
  + نتیجه موفق: کاربر باموفقیت وارد سامانه می‌شود.

**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر**

* روش فراخوانی: پس‌از ورود موفق کاربر به سامانه و ایجاد نشست فعال، در ازای هر درخواست http که از سمت کاربر می‌آید، سامانه وجود انقیاد مشخصه‌ها را با موجودیت فعلی کاربر سنجیده و درصورت بروز عدم تطابق یا عدم انقیاد، نشست کاربر فعلی خاتمه‌می‌یابد.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست.
  + نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد.
  + جزئیات واسط کلاینت: اطلاعاتی ازقبیل نام مرورگر، نسخه‌ی آن و ...
  + متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ...
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + ‌نتیجه: درصورت تغییر مرورگر یا دستگاه کاربر فعال، او از حساب خود خارج می‌گردد.

**مدیریت مشخصه‌های امنیتی**

* روش فراخوانی: کاربر سطح مدیر می‌تواند مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر را ویرایش، حذف یا مشاهده کند. این امکان برای دیگر کاربران فراهم نیست و جلوی آن گرفته می‌شود.

برای مثال می‌تواند به رجوع به بخش "منو > مدیریت کاربران > تعریف کاربران" داده‌های احراز هویت کاربر هدف را ویراسته و ذخیره نماید. درصورت وجود نشست فعال برای کاربر هدف، این نشست خاتمه‌یافته و کاربر مذکور نیازمند ورود مجدد خواهد بود.

* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای تشخیص اینکه آیا این کاربر دسترسی سطح مدیر دارد یا خیر.
  + مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر: داده‌هایی که مدیر می‌تواند آنرا دستخوش تغییر کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی غیرمجاز، کاربر خطای مرتبط دریافت می‌کند.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، نشست کاربری که مشخصه‌های امنیتی او تغییر کرده است، منقضی شده و لازم است تا دوباره به سامانه وارد شود.

**حفظ وضعیت امن در زمان شکست و تحمل خطا**

* روش فراخوانی: هنگام بروز خطای نرم‌افزاری و سخت‌افزاری
* پارامترهای قابل تنظیم:
  + ‌رخداد شکست: هرگونه رخدادی که باعث اختلال در عملکرد سامانه گردد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: وضعیت امن حفظ شده و یک رویداد ممیزی مرتبط با آن که شامل اطلاعات خطای پیش‌آمده است، ثبت می‌گردد. درنهایت شماره‌ی خطای پیش‌آمده به کاربر نمایش‌داده می‌شود تا بعدا قابل ردگیری کاربر باشد.

**انتقال داده‌ی امنیت در داخل محصول**

* روش فراخوانی: ‌أ. در سامانه فعلی تمامی اجزای اجرایی و پایگاه داده درون یک دستگاه کامپیوتر نصب و راه‌اندازی می‌شود. یعنی سامانه یک هسته دارد و monolothic است. درنتیجه داده‌های امنیتی محفوظ می‌مانند.
* پارامترهای قابل تنظیم:
  + داده‌های امنیتی: شامل تمامی داده‌های حساس و حائز اهمیت است.

**محدودیت برروی چندین نشست هم‌زمان**

* روش فراخوانی: کاربر سطح مدیر می‌تواند به رجوع به مسیر "منو > تعاریف > پنل کاربری > تنظیمات لاگین" اقدام به ویرایش تنظیمات محدودیت نشست‌های همزمان کند.
* پارامترهای قابل تنظیم:
  + حد آستانه تعداد نشست‌های همزمان
  + شناسه کاربر: برای شناسایی او و دسترسی‌هایش
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی غیرمجاز به حد آستانه تعداد نشست‌های همزمان، خطایی مرتبط نمایش داده می‌شود و رویداد ممیزی مرتبط ثبت می‌گردد.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن رویه، حد آستانه جدید ذخیره می‌گردد.
  + نتیجه: ثبت رویداد ممیزی مرتبط

**خاتمه دادن به نشست‌ها**

* روش فراخوانی: به خواست خود کاربر و از مسیر "منوی سمت چپ، بالا > خروج" می‌توان از سامانه خارج شد. ویا اگر کاربر به مدت معینی که آن را کاربر مدیر سیستم تعیین می‌کند، بیکار بماند، نشست مرتبط با او خاتمه می‌یابد.
* پارامترهای قابل تنظیم:
  + ‌بازه‌ زمانی مرتبط با خاتمه نشست غیرفعال: عددی که براساس آن سامانه حدود زمانی مجاز برای ماندن درحالت بی‌کار (IDLE) را برای کاربر جایز می‌داند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: درصورت تجاوز از بازه زمانی مذکور، کاربر پیام با مضمون مرتبط دریافت‌کرده و نیازمند ورود مجدد به سامانه است.
  + نتیجه: درصورت فشردن دکمه خروج از حساب، کاربر داوطلبانه به نشست خود خاتمه می‌دهد.

**سوابق دسترسی به محصول**

* روش فراخوانی: کاربر می‌تواند از مسیر "منوی سمت چپ، بالا > تاریخچه فعالیت" به سوابق دسترسی خود دسترسی داشته باشد.
* پارامترهای قابل تنظیم:
  + ‌شناسه کاربر: برای شناسایی او و واکشی سوابق ورود او از پایگاه داده
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: نمایش سوابق ورود موفق و ناموفق

**برقراری نشست**

* روش فراخوانی: ‌کاربر مجاز می‌تواند با مراجعه به مسیر "منو > تعاریف > پنل کاربری > محدودسازی لاگین" تنظیمات مرتبط با محدودسازی ورود را ویرایش‌کند.
* پارامترهای قابل تنظیم:
  + از تاریخ – تا تاریخ: بازه زمانی مجاز برای ورود کاربران را نگه‌می‌دارد.
  + از آی‌پی – تا آی‌پی: بازه نشانی IP مجاز برای ورود کاربران را نگه‌می‌دارد.
  + از پورت – تا پورت: بازه مقادیر پورت مجاز برای ورود کاربران را نگه‌می‌دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی نداشتن به بخش تنظیمات، خطای مرتبط به کاربر نشان‌داده‌می‌شود.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌گردد. نتیجه‌ی این تنظیمات به محدودشدن شرایط ورود کاربر منجر می‌شود.
  + نتیجه: رویداد ممیزی مرتبط ثبت می‌شود.

1. Metadata [↑](#footnote-ref-1)
2. Hash [↑](#footnote-ref-2)
3. Threshold [↑](#footnote-ref-3)