**به نام خدا**

فراخوان دریافت پیشنهاد شرکت‌ها جهت

تحقیق و توسعه محصولات حوزه جلوگیری از نشت داده‌ها

## مقدمه

رشد مستمر اقتصاد دیجیتال کشور اهمیت مقابله با تهدیدات حوزه امنیت اطلاعات را برای سازمان‌های بزرگ بخش خصوصی و دولتی بالا برده است. رویکرد بخش اعظم محصولات و خدمات این حوزه، جلوگیری از نفوذ مهاجمین به شبکه‌های سازمانی است. ولی این رویکرد به تنهایی کافی نیست. امروزه فناوری‌های حوزه «جلوگیری از نشت داده‌ها» یا Data Loss Prevention، نقشی کلیدی در پاسداری از داده‌های حیاتی سازمان‌ها در مقابل تهدیداتی که از درون شبکه سازمانی سرچشمه می‌گیرند ایفا می‌کنند. در این راستا، مرکز فناوری‌های نوظهور ستاد توسعه فناوری‌های اقتصاد دیجیتال و هوشمندسازی معاونت علمی و فناوری ریاست جمهوری از طرح‌های فناورانه جهت تولید محصولات حوزه جلوگیری از نشت داده‌ها در قالب اعطاء تسهیلات بلاعوض و وام حمایت می‎کند. هدف از این طرح:

* حمایت از کسب و کارها و شرکت‌های دانش‌بنیان و فناور
* کاهش مخاطرات تحقیق و توسعه آنها در جهت تولید محصولات و خدمات حوزه امنیت اطلاعات
* حمایت از پژوهشگران و محققان در جهت ارتقاء سطح علمی و پژوهشی بومی می‌باشد.

در این مستند قابلیت‌ها و شاخص‏های عملکردی و غیر عملکردی سیستم DLP مورد نظر، در 17 دسته، تشریح شده است. ذیل هر دسته، قابلیت‌های الزامی، قابلیت‌های افزوده و شاخص‌های عملکرد مربوطه به تفکیک مشخص شده است و لازم است که شرکت‌های پیشنهاد دهنده، در طرح پیشنهادی خود، جزئیات لازم در ارتباط با این قابلیت‏ها و شاخص‏ها را به شرح زیر، در نظر بگیرند:

* پیاده‌سازی قابلیت‌هایی که به عنوان قابلیت‌های الزامی مشخص شده‌اند در محصولات پیشنهادی الزامی است.
* پیاده‌سازی قابلیت‌هایی که به عنوان قابلیت‌های افزوده مشخص شده‌اند ارزش فنی و کسب و کاری محصولات پیشنهادی را افزایش می‌دهد ولی الزامی نیست.
* شاخص‌های عملکرد تعریف شده، برخی از معیارهای کمی و کیفی ستاد را برای ارزیابی و شناسایی محصولات پیشرفته تشریح می‌کنند.

به علاوه در انتها، فهرست برخی استانداردها و مراجع مرتبط این حوزه، که شرکت‏ها جهت ارائه پیشنهاد می‏توانند از آن‏ها بهره بگیرند، آورده شده است.

# تعریف سیاست‌های امنیتی حوزه DLP در سازمان

قابلیت الزامی:

* محصول باید مجموعه‌ای از ابزارهای خاص را برای تعریف و مستند نمودن اهداف و سیاست‌های امنیت اطلاعات سازمان که بر روی مباحث DLP تاثیر گذارند را فراهم آورد.
* محصول باید معیارهای مشخصی را برای اندازه‌گیری درصد انطباق با اهداف و سیاست‌های تعریف شده سازمان در طول زمان، فراهم آورد. این معیارها باید با استفاده از داده‌های جمع‌آوری شده در حین عملکرد سیستم محاسبه شوند.

قابلیت افزوده:

* سیاست‌های امنیتی سازمانی که در سیستم تعریف می‌شوند، باید به صورت مستقیم نحوه عملکرد سیستم را تعیین کنند. به عبارت دیگر، مستند‌سازی سیاست‌های سازمان به صورت متون توصیفی (سیاست‌های دستی) تنها کافی نیست و تعریف این سیاست‌ها به طوری که به صورت خودکار قابل اعمال باشند (سیاست‌های سیستمی)، ارزش افزوده محسوب می‌شود.

شاخص‌های عملکرد:

* تعداد سیاست‌های سیستمی که محصول، قالب‌های از پیش‌ساخته مناسبی برای آنها فراهم می‌آورد.
* توان به روز رسانی و گسترش این قالب‌ها به صورت دوره‌ای توسط تولیدکننده.
* درصدی از کنترل‌های استانداردهای مدیریت امنیت سازمانی مربوطه، مانند ISMS، که توسط قالب‌های سیاست‌های سیستمی محصول پوشش داده می‌شوند.
* درصدی از سیاست‌های سیستمی محصول که توسط محصولات امنیتی دیگر سازمان در قالب یک چارچوبی با قابلیت‏های SOAR، قابل تعیین و کنترل هستند.

# محافظت از «داده‌های در حال سکون» (Data at Rest)

منظور از داده‌های در حال سکون، داده‌هایی است که یا در قالب فایل‌های مختلف روی هاردهای فیزیکی و مجازی و یا در دیتابیس‌های سازمان ذخیره شده‌اند.

قابلیت الزامی:

* محصول باید قابلیت پویش (Scan) فایل‌هایی که در مخازن ذخیره‌سازی فایل‌های سازمانی ذخیره شده‌اند را به صورت آفلاین فراهم آورد، چه از نوع Local Storage و چه از نوع Network Share. منظور از آفلاین این است که محصول در زمانی که کاربر به صورت آنلاین دارد با داده‌های سازمان در سیستم‌های اطلاعاتی سازمانی کار می‌کند، این داده‌ها را پویش نمی‌کند. بلکه بعد از اینکه این داده‌ها توسط نرم‌افزارهای فوق در مخازن ذخیره‌سازی داده‌های سازمانی ذخیره شده‌اند، محصول با توجه به سیاست‌های از پیش تعریف شده، به پویش آن‌ها می‌پردازد.
* محصول باید توان پویش انواع قالب فایل‌های مختلفی را که داده‌های متنی سازمان معمولاً در آن‌ها ذخیره می‌شود را داشته باشد:
	+ Microsoft Office
	+ Open Office
	+ Text
	+ PDF
* محصول باید توان پویش فایل‌های ذخیره شده در سرورهای FTP سازمانی، به خصوص فضای ذخیره‌سازی فایل وب‌سایت‌های سازمانی را داشته باشد.
* محصول باید توان پویش فایل‌ها و داده‌های متنی ذخیره شده در دیتابیس‌های معمول سازمانی را داشته باشد:
	+ MySQL
	+ SQL Server
	+ Oracle
* محصول باید توان پویش فایل‌هایی که در سیستم‌های Collaboration سازمانی معمول ذخیره می‌شوند را داشته باشد:
	+ SharePoint
	+ Mattermost

قابلیت افزوده:

* قابلیت پویش فایل‌های ذخیره شده در سرویس‌های بین‌المللی ذخیره‌سازی ابری سازمانی معمول:
	+ OneDrive
	+ Google Drive
	+ DropBox
* قابلیت پویش فایل‌های ذخیره شده در سرویس‌های ملی ذخیره‌سازی ابری معمول:
	+ ابر آروان
* قابلیت پویش آفلاین انواع فایل‌های دیگر بجز موارد قید شده در قابلیت‏های الزامی.
* قابلیت پویش فایل‌های تصویری با فرمت‌های مختلف برای شناسایی محتواهای متنی.
* قابلیت پویش فایل‌های ذخیره ‌شده در دیگر سرویس‌های بین‌المللی ذخیره‌سازی ابری سازمانی.
* قابلیت پویش فایل‌های ذخیره شده در دیگر سرویس‌های ابری ایرانی.
* قابلیت پویش داده‌های متنی ذخیره شده در انواع دیگر دیتابیس‌ها.
* قابلیت پویش فایل‌های ذخیره شده در دیگر سیستم‌های Collaboration سازمانی.

شاخص‌های عملکرد:

* تعداد فرمت‌های فایل پوشش داده برای هر یک از فناوری‌های فوق.
* مجموع درصدهای سهم بازار محصول ها و سرویس‏های پوشش داده‌شده (یکپارچه‌سازی شده) در کشور در هر یک از حوزه‌های فوق[[1]](#footnote-2).

# محافظت از «داده‌های در حال حرکت» (Data in Motion)

منظور از داده‌های در حال حرکت، داده‌هایی است که بین سیستم‏های مختلف سازمانی انتقال داده می‌شوند و بعد از اینکه داده‌های مذکور انتقال داده شده‌اند، آن‌ها یا تبدیل به داده‌های در حال سکون می‌شوند و یا تبدیل به داده‌های در حال استفاده. بعد از اینکه مجموعه داده‌های خاصی از یک سیستم خارج شدند و قبل از اینکه آن مجموعه به سیستم دیگری برسد و در آن ذخیره شود، داده‌های آن مجموعه به عنوان داده‌های در حال حرکت محسوب می‌شوند.

قابلیت الزامی:

* محصول باید بتواند پروتکل‌های ارتباطی که سیستم‌های مختلف موجود در شبکه‌های سازمانی از آن برای رد و بدل کردن اطلاعات استفاده می‌کنند را شناخته و ترافیکی که بر اساس این پروتکل‏ها منتقل می‏شوند را کنترل نموده و از این طریق، پویش آنلاین و آنی بر روی اطلاعات رد و بدل شده را انجام دهد و داده‌های حساس را از بین آن‏ها شناسایی نماید.
* محصول باید بتواند به صورت آنلاین، داده‌هایی را که از طریق هر بستری توسط سیستم‌های موجود در شبکه سازمان برای هر سیستم خارج از شبکه‌ای ارسال می‌شوند را پویش نماید.
* محصول باید بتواند داده‌هایی را که توسط سیستم‌های سازمانی برای ذخیره‌سازی به مخازن ذخیره‌سازی داده‌های سازمانی ارسال می‌شود را قبل از اینکه آن داده‌ها به آن مخازن برسند، به صورت آنلاین پویش نماید.

شاخص‌های عملکرد:

* درصد نوع ترافیک شبکه معمول سازمانی که توسط محصول پویش می‌شود.

# محافظت از «داده‌های در حال استفاده» (Data in Use) و یکپارچگی با دیگر محصولات و زیرساخت‌های سازمانی

منظور از داده‌های در حال استفاده، داده‌هایی است که سیستم‌های مختلف سازمان به صورت آنلاین با آن‌ها کار می‌کنند و پردازشی بر روی آن‏ها انجام می‏دهند.

در عمل بحث محافظت از «داده‌های در حال استفاده» تنها زمانی امکان پذیر می‌شود که نرم‌افزارهای سازمانی که از آن داده‌ها استفاده می‌کنند یا خود قابلیت‌های DLP را به صورت درونی داشته باشند (Integrated DLP)، یا اینکه DLP سازمان با آن‌ها integrate شوند.

قابلیت الزامی:

* محصول پیشنهادی باید قابلیت integration با نرم‌افزارهایی که با داده‌های سازمانی کار می‌کنند، مانند سرویس ایمیل سازمانی را داشته باشد.
* محصول پیشنهادی باید انواع عملیات Copy/Paste بر روی داده‏های حساس را شناسایی کند.
* محصول پیشنهادی باید Screen Capture از داده‏های حساس را شناسایی کند.
* محصول پیشنهادی باید درخواست چاپ داده‏های حساس را شناسایی کند.

قابلیت افزوده:

* محصول باید توانایی یکپارچگی با انواع و اقسام نرم‌افزارهای سازمانی رایج در کشور را داشته باشد.
* محصول پیشنهادی باید قابلیت پویش آنلاین فایل‌هایی که توسط دستگاه‌های موبایل سازمانی استفاده می‌شوند را داشته باشد.

شاخص‌های عملکرد:

* مجموع درصدهای سهم بازار محصولات و سرویس‏های پوشش داده‌شده (مثلاً سرویس ایمیل مورد پشتیبانی یا نرم افزار اتوماسیون اداری) در کشور در هر یک از حوزه‌های فوق.

# یکپارچگی با انواع DLP های integrated در ابزارها و سیستم‌ها

برخی از نرم‌افزارهای سازمانی که استفاده از آن‌ها در ایران رایج است، مانند Microsoft Office و Google Workspace، دارای قابلیت‌های DLP در محصولات خود هستند. به این نوع قابلیت‌ها، اصطلاحاً Integrated DLP گفته می‌شود.

قابلیت الزامی:

* محصول باید تا حد امکان، از قابلیت‌های DLP موجود در محصولات فوق استفاده نماید.

قابلیت افزوده:

* محصول باید بتواند یک پنل مرکزی برای مدیریت DLP های integrated فراهم آورد.

شاخص‌های عملکرد:

* مجموع درصدهای سهم بازار محصولات Integrated DLP در کشور که توسط محصول DLP پیشنهادی، پشتیبانی می‏شوند.

# یکپارچگی با انواع ابزارها و سیستم‏های محافظتی و تشخیصی امنیت اطلاعات

قابلیت الزامی:

* محصول باید توان یکپارچگی با سیستم‌ SIEM سازمان را داشته باشد.
* محصول باید بتواند لاگ‏هایی در قالب استاندارد تولید و ذخیره سازی کند و قابلیت مدیریت آن لاگ‏ها را نیز فراهم نماید.

شاخص‌های عملکرد:

* مجموع درصدهای سهم بازار محصولات SIEM پوشش داده‌شده (یکپارچه‌سازی شده).

# استفاده از فناوری‌های رمزنگاری

قابلیت الزامی:

* محصول باید برای محافظت از داده‌های سیستمی و داخلی خود، هر جا که مناسب است جهت تأمین قابلیت‏های مورد نظر خود، از فناوری‌های رمزنگاری متقارن و نامتقارن استفاده کند.

قابلیت افزوده:

* یکی از راهکارهای محافظت از نشت داده‌های سازمان، استفاده از الگوریتم‌های رمزنگاری است، گرچه محصولات DLP عموماً خاص رمزنگاری طراحی نمی‌شوند، ولی این گزینه می‌تواند در شرایط خاصی به سازمان‌ها کمک کند. لذا محصول باید این امکان را به سازمان بدهد تا برخی از داده‌های مهم خود را رمز‌گذاری نماید.

شاخص‌های عملکرد:

* تنوع فناوری‌های رمزنگاری که توسط محصول پوشش داده می‌شود.

# تعریف معیارهای شناسایی «داده‌های حساس»

تشخیص این که کدام داده‌ها تحت چه شرایطی از دید سیاست‌های سازمان حساس به شمار می‌روند، یکی از مهم‌ترین قابلیت‌های هر سیستم DLP است.

قابلیت الزامی:

* محصول باید توان تعریف دقیق معیارهای شناسایی داده‌های حساس را به مدیران سیستم بدهد.
* محصول باید بتواند موارد زیر را در داده‌های پویش شده تشخیص دهد:
	+ رشته‌های متنی مشخص،
	+ رشته‌هایی که از الگوهای Regex خاص پیروی می‌کنند.
* محصول باید بتواند بستگی به context فایل یا سیستمی که داده‌های فوق در آن مشاهده شده‌اند، در مورد حساس بودن یا نبودن آن‌ها تصمیم بگیرد. مثلاً، یک سری داده‌ها اگر در فایل‌های یک پوشه خاص مشاهده شوند، مشکلی ندارد، ولی اگر فایل‌های حاوی آن داده‏ها در پوشه‌های دیگری باشند، از دید سازمان مشکل امنیتی به حساب می‌آید. یا اینکه وجود یک سری داده‌ها در ایمیلی که توسط یک کاربر خاص ارسال می‌شود مشکلی ندارد، ولی همان داده‌ها نباید توسط کاربران دیگر ایمیل شود.

قابلیت افزوده:

* محصول باید توانایی شناخت الگوهای غنی تری به جز pattern-matching ساده هم داشته باشد: مثلاً شاید وجود یک شماره پرسنلی تکی در یک متن خاص مشکل‌ساز نباشد، ولی یک لیست از شماره‌های پرسنلی در همان context حساس به شمار آید.

شاخص‌های عملکرد:

* تنوع قالب‌های از پیش‌ساخته شده برای شناسایی داده‌های حساس.
* استفاده از یک business rule engine برای تعریف معیارهای شناسایی داده‌های حساس.
* استفاده از machine learning برای شناسایی داده‌های حساس.

# توانایی شناخت سازمان و داشتن هوش سازمانی در شناسایی داده‌های حساس

منظور از هوش سازمانی، آگاهی یک محصول به ساختار و فرآیندهای سازمانی یک سازمان خاص است. هر چقدر یک محصول DLP درک عمیق‌تری از کسب و کار یک سازمان داشته باشد، از قدرت تشخیص بیشتری برای شناسایی داده‌های حساس سازمان برخوردار خواهد بود.

قابلیت الزامی:

* محصول باید قابلیت یکپارچگی با سیستم Active Directory را در سازمان‌هایی که از آن استفاده می‌کنند، داشته باشد تا قوانین دسترسی پیاده‌سازی شده توسط Active Directory را در شناسایی داده‌های حساس مد نظر قرار دهد.

قابلیت افزوده:

* محصول باید با سیستم منابع انسانی سازمان یکپارچه باشد تا در تشخیص اجازه دسترسی افراد به داده‌های مختلف، موقعیت سازمانی آن‌ها را نیز مد نظر قرار دهد.
* محصول باید با سیستم‌هایی که فرآیندهای سازمانی را در سازمان پیاده‌سازی نموده‌اند یکپارچگی داشته باشد تا بتواند حساسیت یا عدم حساسیت داده‌های متنی را در context فرآیندهای سازمانی مربوطه شناسایی نماید.

شاخص‌های عملکرد:

* قابلیت یکپارچگی با یک پلتفرم Security Intelligence Platform.
* قابلیت یکپارچگی با یک پلتفرم GRC.
* قابلیت یکپارچگی با یک پلتفرم با قابلیت‏های SOAR.

# تعریف گزینه‌های کاربران در مواجه با داده‌های حساس

هر زمان که محصول داده‌های حساس سازمانی را بعد از پویش آفلاین یا آنلاین داده‌ها شناسایی نمود، باید گزینه‌های مناسب برای واکنش نسبت به آن را فراهم نماید. مثلاً سیستم DLP می‌تواند به یک کاربر خاص اطلاع دهد که فایلی که او قصد دارد ایمیل کند حاوی اطلاعاتی است که شاید حساس باشد. در این صورت، کاربر امکان دارد از ارسال فایل خودداری کند، فایل را ویرایش کند تا اطلاعات حساس را حذف کند، یا به سیستم DLP اطلاع دهد که با مسئولیت خود کاربر، سیستم باید اجازه ارسال فایل را صادر کند.

قابلیت الزامی:

* محصول باید به کاربر اجازه دهد در صورت امکان داده‌های مربوطه را حذف یا مخدوش (Redact) یا جایگزین و یا قرنطینه کند یا اینکه با ذکر دلیل اجازه دهد داده‌ها ذخیره یا منتقل شوند.
* محصول باید به صورت شفاف به کاربر توضیح دهد که ذخیره یا انتقال این داده‌هایی که حساس شناسایی شده‌اند دقیقاً کدام سیاست‌های سازمانی را نقض می‌کند و گزینه‌های مناسبی که سیاست‌های سازمانی در شرایط حاضر در اختیار کاربر قرار می‌دهند را برای وی تشریح نماید.

قابلیت افزوده:

* در مواردی که کاربر مطمئن نیست چه واکنشی مناسب است، محصول باید یک فرآیند سازمانی برای کسب تکلیف از مقامات بالاتر سازمانی را برای کاربر فراهم آورد.

# وجود قابلیت‌های مدیریت سیستم

همانطور که پیش تر شرح داده شد، گزینه‏های مختلف واکنشی در هنگام تشخیص داده‏های حساس، باید توسط کاربران سازمانی قابل انتخاب و اعمال باشندولی در برخی از شرایط، سیستم نیاز دارد که فردی که نقش مدیر سیستم (System Administrator) را ایفا می‌کند، اقدام خاصی انجام دهد. مثلاً زمانی که کاربر مثال پاراگراف قبل با مسئولیت خود اقدام به ارسال یک فایل خاص می‌کند، بعداً یکی از مدیران سیستم باید گزارشی در این مورد دریافت کند و فرصت بررسی صحت تصمیم کاربر را داشته باشد. یا زمانی که سیستم DLP تعدادی فایل حساس را از طریق پویش آفلاین در جایی پیدا می‌کنند که آن فایل‌ها نباید باشند، یک مدیر سیستم است که باید به سیستم بگوید با آن فایل‌ها چگونه باید برخورد شود.

هر سیستم DLP نیاز دارد یک پنل مدیریتی برای انجام عملیات مدیریت سیستمی فراهم آورد.

قابلیت الزامی:

* قابلیت انجام همه کارهایی که مدیران سیستم نیاز به انجام آن را دارند باید از طریق یک سیستم واسط کاربری شفاف و منطقی در دسترس کاربران مربوطه قرار بگیرد.
* سیستم باید گزارش‌های قدرتمندی را به صورت آنلاین در اختیار مدیران سیستم قرار دهد تا آن‌ها را در انجام وظایف خود یاری نماید.

قابلیت افزوده:

* سیستم باید یک گزارش ساز در اختیار مدیران سیستم قرار دهد تا هر گزارشی را که نیاز دارند را بتوانند برای استفاده کاربران مربوطه طراحی و تولید کنند.

شاخص‌های عملکرد:

* وجود قابلیت‌های یکپارچه برای تحلیل‌های عملیاتی با استفاده از ابزارها فناوری‌های business intelligence.
* وجود قابلیت‌های یکپارچه برای تحلیل‌های عملیاتی با استفاده از ابزارها فناوری‌های data science.
* وجود قابلیت‌های یکپارچه برای تحلیل‌های عملیاتی با استفاده از ابزارها فناوری‌های machine learning.

# آینده‌نگری در انتخاب معماری و فناوری‌های پایه محصول

عملکرد کارآمد محصولات DLP و توانایی آن‏ها برای به روز شدن و به روز ماندن در طی زمان، به استفاده از مجموعه تکنولوژی‌های روز IT در دنیا و نحوه بکارگیری آن‏ها وابسته است و باید همواره همراه با رشد و تغییر دیگر تکنولوژی‌ها، تغییر و توسعه یابد.

قابلیت الزامی:

* معماری محصول و فناوری‌های نرم‌افزاری که در تولید محصول به کار رفته‌اند، باید توان رشد مستمر قابلیت‌های محصول و یکپارچگی با آخرین محصولات سازمانی را روی پلتفورم‌های مختلف سخت افزاری و سیستم‌های عامل مربوطه فراهم آورد.

شاخص‌های عملکرد:

* استفاده از معماری‌های micro services و serverless

# استفاده از پروژه‌های متن باز

پروژه‌های موجود متن باز در زمینه DLP (Open DLP و MyDLP) بسیار قدیمی هستند و سال‌ها است که توسعه آن‌ها ادامه پیدا نکرده است.

قابلیت الزامی:

* استفاده از پروژه‌های متن باز تنها برای مراحل تحقیق و توسعه و نمونه سازی اولیه محصول قابل پذیرش است.
* در صورت قصد تولید کننده محصول برای استفاده از هر یک از این پروژه‌ها در دراز مدت، تولید کننده موظف است که ثابت کند که (1) کاملاً به کد پروژه تسلط دارد و توانایی توسعه آن را دارا است و (2) یک نقشه راه منطقی برای تضمین استمرار توسعه پروژه را در دراز مدت در دست اجرا دارد.

قابلیت افزوده:

* محصول نباید از پروژه‌های متن باز فوق استفاده کند.

شاخص‌های عملکرد:

* درصدی از کد محصول که توسط تولید‌کننده به صورت open source در اختیار بازار قرار می‌گیرد.

# فرآیند تولید

به خاطر نقش حیاتی‌ای که DLP در اکوسیستم هر سازمان ایفاء می‌کند، کیفیت محصولات DLP باید در بالاترین سطح ممکن باشد. بخش مهمی از این امکان به کیفیت فرآیند تولید محصول باز می‌گردد.

قابلیت الزامی:

* تولید کننده باید از متدلوژی‌ و ابزارهای نوین توسعه و نگهداری محصولات نرم‏افزاری استفاده نماید.
* تولید کننده باید مستندات لازم در مورد فرآیند تولید محصول و استانداردهای مربوطه را ارائه نماید.

شاخص‌های عملکرد:

* استفاده از متدلوژی‌های Agile که به Extreme Programming نزدیک‌تر هستند تا به Scrum.
* استفاده از رویکرد TDD یا مشابه.
* استفاده از رویکرد DDD یا مشابه.

# فرآیند تضمین کیفیت

به خاطر نقش حیاتی‌ای که DLP در اکوسیستم هر سازمان ایفاء می‌کند، کیفیت محصولات DLP باید در بالاترین سطح ممکن باشد. بخش مهمی از این امکان به فرآیند تضمین کیفیت محصول باز می‌گردد.

قابلیت الزامی:

* تولید کننده باید مستندات لازم در مورد فرآیند تست و تضمین کیفیت محصول و استانداردهای مربوطه را ارائه نماید.

شاخص‌های عملکرد:

* درصد پوشش کد محصول توسط unit test های خودکار.
* درصد پوشش functionality های سیستم توسط تست‌های QA خودکار.

# سرعت و عملکرد سیستم

به خاطر نقش حیاتی‌ای که DLP در اکوسیستم هر سازمان ایفاء می‌کند، سرعت و عملکرد محصولات DLP باید در بالاترین سطح ممکن باشد.

قابلیت الزامی:

* تولید کننده باید مستندات لازم در مورد رویکرد شرکت برای تضمین سرعت و عملکرد محصول و استانداردهای مربوطه را ارائه نماید.

شاخص‌های عملکرد:

* وجود یک test bed برای اجرا، اندازه‌گیری، ثبت و مقایسه نتایج انواع تست‌های سرعت و عملکرد محصول.

# شاخص‌های عملکرد عمومی

* وجود یک مدل کسب و کار که اجازه می‌دهد شرکت‌های ثالث اقدام به تولید ماژول‌های افزودنی‌های مختلف برای محصول نمایند.
* تعداد ماژول‌های افزودنی‌های تولید شده توسط شرکت‌های ثالث.
* تعداد تیم‌های دانشگاهی که در طراحی و تولید محصول یا ماژول‌های افزودنی برای آن مشارکت دارند.

# استانداردها و مراجع کمکی

استانداردهای مختلفی در دنیا برای بیان نیازمندی‌های امنیتی DLP تدوین شده‌اند که برخی از آنها به صورت مستقیم برای DLP نوشته شده و برخی دیگر به مجموعه‌‌ بزرگتری از مسائل امنیتی اشاره دارند که فروشندگان مطرح DLP از آنها برای بیان نیازمندی‌ها و سیاست‌های DLP خود استفاده کرده‌اند. در زیر برخی از آنها آورده شده‌اند که شرکت‌کنندگان در این فراخوان می‌توانند ها جهت ارائه پیشنهاد از آن‏ها بهره بگیرند.

* استاندارد NIST 800-171 [1]
* گزارشی با عنوان "Data Loss Prevention" از موسسه [2] SANS
* چک لیستی با عنوان " Data Loss Prevention " از موسسه SANS [3]
* گزارشی با عنوان " SecaaS Implementation Guidance, Category 2: Data Loss Prevention" از موسسه CSA [4]
* نمایه حفاظتی (Protection Profile) مطابق با استانداردISO 15408 با عنوان " Common Criteria Requirement of Data Leakage Protection System " [5]و [6]
* هدف امنیتی (Security Target) مطابق با استانداردISO 15408 از Symantec [7]،RSA [8] و McAfee [9]

## مراجع

[1] <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>

[2] <https://www.sans.org/reading-room/whitepapers/dlp/paper/32883>

[3] [https://www.sans.org/reading-room/whitepapers/analyst/data-protection-requirements-checklist-34780/RK=2/RS=oEzqXU70mo8iB7umbOFtnnScQrw-](https://www.sans.org/reading-room/whitepapers/analyst/data-protection-requirements-checklist-34780/RK%3D2/RS%3DoEzqXU70mo8iB7umbOFtnnScQrw-)

[4] [https://cloudsecurityalliance.org/artifacts/secaas-category-2-data-loss prevention-implementation-guidance/](https://cloudsecurityalliance.org/artifacts/secaas-category-2-data-loss%20prevention-implementation-guidance/)

[5] <https://link.springer.com/chapter/10.1007/978-3-642-27142-7_37>

[6] [https://silo.tips/download/common-criteria-requirement-of-data-leakage protection-system](https://silo.tips/download/common-criteria-requirement-of-data-leakage%20protection-system)

[7] <https://www.commoncriteriaportal.org/.../SYMC%20DLP%20EAL2%20Security%20Target%20v1-0.pdf>

[8] <https://www.commoncriteriaportal.org/files/.../rsa-dataloss-v65-sec-eng.pdf>

[9] [https://www.commoncriteriaportal.org/.../383-4-342%20MFE%20DLPe%209 -4%20ST.pdf](https://www.commoncriteriaportal.org/.../383-4-342%20MFE%20DLPe%209%20-4%20ST.pdf)

1. بدین معنا که قابلیت یکپارچه شدن با محصولات رایج در کشور، امتیاز بیشتری نسبت به قابلیت یکپارچه سازی با محصولات متفرقه دارد. [↑](#footnote-ref-2)