


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ


فهرست مطالب

- 1..... مقدمه
- 2..... 1 خدمات مدیریتی افتا
- 2..... 1-1 مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات
- 2..... 1-3 مشاور مادر طرح امن سازی
- 2..... 1-4 ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات
- 3..... 2- خدمات فنی افتا
- 3..... 2-1 نصب و پشتیبانی امنیتی محصولات افتا
- 5..... 3- خدمات آموزشی افتا
- 5..... 4 خدمات عملیاتی افتا
- 6..... 4-1 آزمون و ارزیابی امنیتی
- 6..... 4-2 کشف نقص امنیتی
- 7..... 4-3 پیاده سازی مرکز عملیات امنیت و تیم پاسخ به رخداد
- 7..... 4-4 راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد
- 7..... 4-5 امن سازی و مقاوم سازی سامانه ها، زیرساختها و سرویسها
- 8..... 4-6 پیاده سازی امنیت فیزیکی و محیط پیرامونی

تاریخ سند: فروردین 1402	<h2>معرفی خدمات افتا</h2>	 مرکز مدیریت راهبردی افتا
شناسه :		
صفحه 1 از 9		

مقدمه

با توجه به گستردگی خدمات در حوزه فناوری اطلاعات و امنیت فناوری اطلاعات و درهم تنیدگی‌های موجود که باعث ابهام در تمییز خدمات افتایی می‌شود، سند جاری با هدف معرفی خدماتی که در زمان تدوین این سند تحت پوشش گواهی‌های افتا می‌باشند تدوین شده است. در این سند علاوه بر عنوان و تعریف خدمات افتا، اسناد تکمیلی تدوین شده برای گرایش‌های مختلف آدرس‌دهی شده است. این اسناد شامل اسناد معرفی، الزامات و دستورالعمل‌ها، راهنماهایی می‌باشد که لازم است در هر زمان با مراجعه به وبسایت افتا، آخرین نسخه منتشر شده از این اسناد مورد بهره‌برداری قرار بگیرد.

تاریخ سند: فروردین 1402	<h1>معرفی خدمات افتا</h1>	 <p>مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 2 از 9		

1- خدمات مدیریتی افتا

منظور از خدمات مدیریتی افتا، خدماتی از جنس طراحی‌های کلان و ساختاری، طرح‌ریزی، برنامه‌ریزی، بهبود و ساماندهی، سنجش و پیشگیری مخاطرات امنیتی در سازمان‌ها و تدوین نظام‌ها و سیاست‌های امنیتی و ممیزی انطباق با استانداردهای موجود در این حوزه‌هاست.

1-1- مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات

در حالت کلی مشاوره استقرار سیستم مدیریت امنیت اطلاعات (ISMS)، سیستم مدیریت تداوم کسب و کار (BCM)، سیستم مدیریت بازیابی پس از فاجعه (DRM)، سیستم مدیریت مخاطرات (RM)، سیستم مدیریت رخدادهای (IM) و مانند آنها در حوزه تعریف این خدمت می‌گنجند.

اما در حال حاضر با توجه به اینکه دارندگان این پروانه صرفاً از لحاظ توانمندی مشاوره استقرار سیستم مدیریت امنیت اطلاعات احراز صلاحیت شده‌اند، صدور پروانه تنها برای این استاندارد انجام می‌پذیرد. دارنده این پروانه موظف است در هر یک از گام‌های پروژه استقرار سیستم مدیریت امنیت اطلاعات از ابتدا (تعیین دامنه) تا مراحل پایانی (آماده‌سازی برای ممیزی شخص ثالث/ آموزش و آگاهی‌رسانی) بر اساس سند «الزامات استقرار سیستم مدیریت امنیت اطلاعات» که در وبسایت مرکز افتا منتشر شده است، ایفای نقش نماید.


یادآور می‌شود که مسئولیت اصلی استقرار سیستم مدیریت امنیت اطلاعات در یک سازمان برعهده مدیریت ارشد آن سازمان است و رعایت مفاد سند مذکور و نیز سند «راهنمای تعیین دامنه» می‌تواند در اجرای مسئولیت‌های کارفرما تاثیر بسزایی داشته باشد.

1-2- مشاور مادر طرح امن سازی (اپراتور امنیت)

"مشاور مادر طرح امن سازی" متولی اجرای طرح امن سازی در زیرساخت‌های حیاتی کشور خواهد بود.

1-3- ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات

این گرایش در حال حاضر متمرکز بر ممیزی انطباق با استاندارد ISO 27001 و در صورت احراز صلاحیت از نظر ممیز، توصیه ممیزی شونده به مرکز افتا برای دریافت گواهینامه ملی انطباق با این استاندارد می‌باشد. شایان ذکر است که بر اساس گزارش ممیزی ارائه شده به کمیته تخصصی مرتبط در مرکز افتا، در خصوص وضعیت نهایی انطباق ممیزی شونده با ISMS تصمیم‌گیری می‌شود.


تاریخ سند: فروردین 1402	<h2>معرفی خدمات افتا</h2>	 <p>مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 3 از 9		

2- خدمات فنی افتا

2-1- نصب و پشتیبانی امنیتی محصولات افتا

کاربرد این پروانه فعالیت تنها در قراردادهایی است که کارفرما با رعایت موارد بیان شده در این سند یک محصول فتایی را به همراه خدمات نصب و پشتیبانی آن خریداری می‌کند. به عبارت دیگر خدمات نصب و پشتیبانی محصولات فتا شامل فعالیت‌های زیر است:

- فروش، نصب و راه‌اندازی اولیه محصولات
 - پشتیبانی و نگهداری محصولات شامل
 - پشتیبانی فنی، ضمانت، عیب‌یابی، رفع نقص‌ها و باگ فیکس، نگهداری زمانبندی شده (مدت دار مثلا ماهیانه)
 - انواع بروزرسانی‌ها اعم از بروزرسانی وصله‌ها، بروزرسانی محتوای امنیتی و بروزرسانی نسخه محصول
 - خدمات جایگزینی و تعمیر سخت‌افزار
 - آموزش استفاده و چگونگی راهبری محصول
- در واقع این پروانه در حال حاضر صرفاً برای پشتیبانی محصولات داخلی دارای گواهی ارزیابی امنیتی محصولات و آن دسته از محصولات خارجی فاویبی که مشابه داخلی ندارند صادر می‌شود.
- لازم به ذکر است فعالیت‌های زیر در حوزه پوشش این پروانه نمی‌گنجند و شرکت‌های ارائه دهنده این خدمات لازم است برای پروانه امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها اقدام کنند:
- پشتیبانی و نگهداری شبکه OT/IT ،
 - مشاوره و طراحی شبکه،
 - طراحی و مشاوره امنیت شبکه،

تاریخ سند: فروردین 1402	<h2>معرفی خدمات افتا</h2>	 <p>مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 4 از 9		

– نصب، راه اندازی و پشتیبانی محصولات حوزه مدیریت شبکه و تامین امنیت شبکه (از قبیل انواع فایروال /

فایروال نسل بعدی، سامانه های تشخیص و جلوگیری از نفوذ، ابزارهای پایش شبکه، محصولات مدیریت

امنیت داده، محصولات مدیریت دسترسی تحت شبکه، محصولات مدیریت آسیب پذیری و وصله ها،...)

در حال حاضر در وبسایت مرکز افتا اسناد مربوط به این گرایش به شرح ذیل منتشر شده است:

– حوزه صنعتی:

○ «دستورالعمل امنیت اطلاعات سیستم های مانیتورینگ ایستگاه های گاز»


○ «الزامات امنیتی عملیاتی زیرساخت های حیاتی صنعتی»

– محصولات نرم افزاری:

○ الزامات امنیتی ارائه محصولات نرم افزاری سازمانی به زیرساخت های حیاتی

○ الزامات امنیتی زیرساخت های حیاتی در استفاده از محصولات نرم افزاری سازمانی

دسته بندی تعیین شده محصولات برای این پروانه در حال حاضر به شرح ذیل است:

تاریخ سند: فروردین 1402	<h2>معرفی خدمات افتا</h2>	 <p>مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 5 از 9		


- سامانه‌های اسکادا
- سامانه‌های کنترل محلی و DCS
- زیرساخت‌های اندازه‌گیری پیشرفته
- تجهیزات شبکه (از قبیل سویچ، روتر، سرور، تجهیزات ذخیره‌سازی و پشتیبان‌گیری)
- محصولات ضدبدافزار/ محافظت از نقطه‌نهایی
- تجهیزات رمزنگاری (VPN, Token, HSM)
- سامانه‌های نرم‌افزاری (سامانه‌های نرم‌افزاری بومی دارای گواهی ارزیابی امنیتی محصولات افتا که در هیچ یک از دسته‌بندی‌های دیگر نباشند که صدور پروانه برای آنها صرفاً برای تک‌محصول دارای گواهی ارزیابی امنیتی انجام می‌شود).

3- خدمات آموزشی افتا

این حوزه خدمات شامل ارائه آموزش کلیه دوره‌های امنیتی در سطوح و موضوعات مختلف به متقاضیان است. دامنه این حوزه مربوط به آموزش‌هایی می‌باشد که منجر به دریافت گواهینامه‌های ملی و بین‌المللی در زمینه دوره‌های آموزشی امنیت اطلاعات و ارتباطات گردد. در حال حاضر مشخصات دوره‌های آموزشی مورد تایید افتا در قالب سند «معرفی دوره‌های آموزشی افتا» در وبسایت مرکز افتا منتشر شده است.

4- خدمات عملیاتی افتا

خدمات عملیاتی افتا، بیشتر بر مهارت‌های خاص و فنی کارشناسان برای پیاده‌سازی و یا حصول اطمینان از عملکرد مناسب کنترل‌های پیاده‌سازی شده تاکید دارد. در واقع تمرکز اصلی این گرایش اقدامات عملیاتی امنیتی است که توسط کارشناسان این حوزه برای پایش، ارزیابی و ارتقاء سطح امنیت انجام می‌پذیرد و معمولاً برخلاف گرایش نصب و پشتیبانی، مبتنی بر محصول/گروه محصول خاصی نیست.

تاریخ سند: فروردین 1402	 <p style="text-align: center;">معرفی خدمات افتا</p> <p style="text-align: center;">مرکز مدیریت راهبردی افتا</p>
شناسه :	
صفحه 6 از 9	

1-4- آزمون و ارزیابی امنیتی

خدمت آزمون و ارزیابی امنیتی شامل کلیه خدمات ارزیابی امنیتی نرم افزار، تجهیزات، سرویس ها و سامانه ها، آزمون نفوذپذیری و آزمون آسیب پذیری می باشد. در واقع اگر نیاز به یکی از فعالیت های زیر باشد، این پروانه می بایست مورد استفاده قرار بگیرد:

- پوشش آسیب پذیری سامانه ها و شبکه IT/OT
- ارزیابی آسیب پذیری سامانه، تجهیزات و سرویس ها
- آزمون نفوذپذیری سامانه، تجهیزات و سرویس ها
- ارزیابی امنیتی سامانه، تجهیزات و سرویس ها


شایان ذکر است که دارندگان این پروانه اجازه ارزیابی امنیتی محصول و صدور تاییدیه امنیتی برای آن را ندارند. در حال حاضر سند «الزامات دارندگان پروانه فعالیت خدمت آزمون و ارزیابی در اجرای پروژه های آزمون نفوذپذیری» در وبسایت مرکز افتا منتشر شده است.

2-4- کشف نقص امنیتی

کشف نقص امنیتی خدمتی است که در آن سامانه/سامانه های کارفرما توسط هکرها تست نفوذ می شود. مدیریت این خدمت توسط چارچوبی که پلتفرم باگ بانته نامیده می شود و در اختیار شرکت متقاضی پروانه می باشد، انجام می پذیرد. باگ بانته به دو صورت زیر قابل انجام است:

- باگ بانته عمومی : که در آن مشتری سامانه ای را برای تست نفوذ معین می کند که دسترسی به آن از طریق اینترنت برای عموم آزاد می باشد.
- باگ بانته خصوصی : که در آن مشتری سامانه ای را برای تست نفوذ معین می کند که دسترسی به آن برای عموم آزاد نبوده و نیاز به مجوز خاصی دارد (به عنوان نمونه سامانه در روی شبکه محلی قرار دارد و یا از طریق VPN قابل دسترس است). همچنین در شرایط خاص ممکن است مشتری درخواست کند که برای سامانه ای که در دسترس عموم قرار دارد، تست نفوذ از مسیر مشخصی تحت مالکیت شرکت برگزار کننده مسابقه انجام پذیرد.

در خدمت «مسابقات کشف نقص امنیتی»، مشتری سامانه ها و سرویس های خود را در قالب نام دامنه و آدرس IP به شرکت دارای پروانه فعالیت در این گرایش اعلام می کند و شرکت با برگزاری مسابقه در محدوده آزمون نفوذ مشخص شده توسط مشتری، نقص های کشف شده توسط شرکت کنندگان در مسابقه را ارزیابی و در صورت صحت به اطلاع مشتری می رساند تا اقدامات لازم برای رفع آن صورت پذیرد. همچنین بر اساس سطح نقص گزارش شده، جوایزی از طرف مشتری به کشف کننده نقص مذکور تعلق می گیرد.

تاریخ سند: فروردین 1402	<h2 style="margin: 0;">معرفی خدمات افتا</h2>	 <p style="margin: 0;">مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 7 از 9		

در حال حاضر اطلاعات این گرایش در قالب سند «معرفی خدمت مسابقات کشف نقص امنیتی» در وبسایت مرکز افتا منتشر شده است.

3-4- پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد

خدمات مرتبط با پیاده‌سازی مرکز عملیات امنیت به خدماتی اطلاق می‌شود که وظیفه راه‌اندازی و پشتیبانی از تجهیزات و سامانه‌های مرتبط با مرکز عملیات امنیت (از قبیل سامانه‌های مدیریت یکپارچه تهدیدات، سامانه‌های مدیریت رخدادها و حوادث امنیتی) را برعهده دارد و برای طراحی ساختار، ارائه راهکارهای مقابله با حوادث امنیتی، تدوین فرایندهای مرتبط، استقرار استانداردهای مرتبط و آموزش کاربران مرکز عملیات امنیت در محیط کارفرما مورد استفاده قرار می‌گیرد. در واقع پیاده‌سازی مرکز عملیات امنیت شامل سه بعد فرآیندها (رویه‌ها)، تجهیزات و آموزش نیروی انسانی می‌باشد.

خدمات مرتبط با پاسخ به رخدادهای سایبری به خدماتی اطلاق می‌شود که به منظور شناسایی حوادث امنیتی و سایبری رسیدگی به موقع به آنها مورد استفاده قرار می‌گیرد. متقاضیان این پروانه می‌بایست مجموعه‌ای از کارشناسان متخصصی در هر دو موضوع را دارا باشند.

4-4- راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد

خدمات مرتبط با راهبری مرکز عملیات امنیت به خدماتی اطلاق می‌شود که به منظور راهبری سامانه‌های مرکز عملیات امنیت، پایش و تحلیل رخدادهای امنیتی، تهیه و تدوین گزارش‌های رخدادهای امنیتی و رسیدگی به موقع به آنها در محیط کارفرما، مورد استفاده قرار می‌گیرد.

5-4- امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها (IT)

این خدمت به فعالیت‌هایی در خصوص امن‌سازی و مقاوم‌سازی شبکه، سامانه‌ها، سرویس‌ها و تجهیزات نرم‌افزاری و سخت‌افزاری می‌پردازد. این گرایش شامل خدمات ذیل می‌باشد:

- پیکربندی امن: این زیر گرایش شامل فعالیت‌ها در حوزه نصب و پشتیبانی محصولات امنیت شبکه می‌باشد. با توجه به آنکه نصب و پشتیبانی محصولات امنیت شبکه نیاز به دانش امنیتی و امن‌سازی (علاوه بر دانش تخصصی محصولات قابل پشتیبانی) دارد، نصب و پشتیبانی این نوع از محصولات نیاز به این گواهی دارد.



مرکز مدیریت راهبردی افتا

معرفی خدمات افتا

تاریخ سند: فروردین 1402

شناسه :

صفحه 8 از 9

- امن سازی شبکه های فناوری اطلاعات (IT): ارائه دهنده این زیر گرایش، نسبت به امن سازی و مقاوم سازی شبکه، سامانه، سرویس، تجهیزات نرم افزاری و سخت افزاری برای مقابله با بدافزارها و دسترسی های غیرمجاز، در محیط کارفرما اقدام می نماید.

4-6- امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها (OT)

این خدمت به فعالیتهایی در خصوص امن سازی و مقاوم سازی شبکه، سامانه ها، سرویس ها و تجهیزات صنعتی می پردازد و شامل زیر گرایش های ذیل می باشد:

- پیکربندی امن محصولات صنعتی: این حوزه دربردارنده فعالیتهایی در خصوص نصب سامانه های امنیتی در حوزه زیرساخت های صنعتی نظیر دیتا دیود صنعتی، پیشگر شبکه صنعتی، انواع لاگر، فایروال صنعتی، نرم افزار Whitelist، مدیریت یکپارچه به روزرسانی در سطح فیلد و... می باشد.

- مشاوره امن سازی و مقاوم سازی زیرساخت صنعتی: این حوزه دربردارنده فعالیتهایی در خصوص وضعیت امنیت سایبری زیرساخت صنعتی را به صورت غیرفعال¹ ارزیابی و برای ارتقا آن راه حل ارائه دهند. دارندگان این نوع پروانه اجازه انجام عملیات فعال و ایجاد تغییراتی نظیر نصب نرم افزار، افزودن تجهیز جدید و... در زیرساخت صنعتی را ندارند.


- امن سازی شبکه های صنعتی: در این زیرگرایش، شرکت ارائه دهنده خدمت اقدام به امن سازی و مقاوم سازی سامانه های کنترل صنعتی برای مقابله با بدافزارها و دسترسی های غیرمجاز، در محیط کارفرما می نماید. این سامانه ها شامل کلیه نرم افزارها، سخت افزارها و سایر عوامل مرتبطی هستند که به منظور اندازه گیری الکترونیکی، کنترل، مانیتورینگ، عیب یابی و ایمنی فرآیندهای صنعتی تولیدی، انتقالی و توزیعی به کار گرفته می شوند.

4-7- پیاده سازی امنیت فیزیکی و محیط پیرامونی

این گرایش شامل طراحی، نصب، پیکربندی و پشتیبانی از راه حل های ایجاد امنیت فیزیکی و محیط پیرامونی است. پروژه هایی با ماهیت طراحی و پیاده سازی راهکارهای امنیت محیط پیرامونی از جمله موارد ذیل در دامنه این پروانه قرار می گیرد:

- طراحی و پیاده سازی راهکارهای امنیت محیط پیرامونی و پایش تصویری

¹ Passive

تاریخ سند: فروردین 1402	<h2>معرفی خدمات افتا</h2>	 <p>مرکز مدیریت راهبردی افتا</p>
شناسه :		
صفحه 9 از 9		

- طراحی و پیاده‌سازی سامانه‌های اطفای حریق در محیط‌های مرتبط با فناوری اطلاعات
 - طراحی و پیاده‌سازی راه‌حل‌های تامین مطمئن انرژی برای تجهیزات فناوری اطلاعات
 - طراحی و پیاده‌سازی سامانه‌های کنترل دسترسی فیزیکی مانند سیستم‌های کنترل ورود/خروج
- در حال حاضر این پروانه صرفاً برای زیر گرایش " طراحی و پیاده‌سازی راهکارهای امنیت محیط پیرامونی و پایش تصویری" صادر می‌شود.