بسمه تعالی

آیین‌نامه ساماندهی خدمات افتا

سازمان فناوری اطلاعات ایران

و

مرکز مدیریت راهبردی افتا

سال ۱۳۹۵

نسخه	تعداد صفحات	تاریخ ویرایش
۱,۰	۹	۱۳۹۳/۰۶/۲۹
۲,۰	۲۱	۱۳۹۵/۰۶/۱۳
مرجع: استاندارد NIST SP 800-35		

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

فهرست

۱. مقدمه

این آیین‌نامه بر اساس تبصره یک ماده ۲۳۱ قانون برنامه پنج‌ساله پنجم با هدف ساماندهی ارائه خدمات امنیت فضای تولید و تبادل اطلاعات (افتا) از طریق صدور پروانه فعالیت، تدوین گردیده است. این آیین‌نامه دربردارنده‌ی نحوه صدور پروانه فعالیت ارائه‌کنندگان خدمات در حوزه‌های افتا، به همراه بیان نقش‌های ارائه‌کنندگان خدمات، دریافت‌کنندگان خدمات، مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران به‌عنوان صادرکننده پروانه فعالیت، می‌باشد.

۲. قلمرو

۲,۱ قلمرو این آیین‌نامه در محدوده مرزهای جغرافیایی کشور جمهوری اسلامی ایران می‌باشد.

۲,۲ قلمرو دریافت‌کنندگان خدمات افتا کلیه مشمولین ماده «۲۲۲» و بند «الف» ماده «۲۳۱» قانون برنامه پنجم توسعه جمهوری اسلامی ایران می‌باشند.

۲,۳ قلمرو خدمات افتا، کلیه خدمات دسته بندی شده در پیوست یک این آئین نامه می‌باشد.

۳. تعاریف

۱,۳ افتا: امنیت فضای تولید و تبادل اطلاعات.

۲,۳ . سازمان: سازمان فناوری اطلاعات ایران.

۳,۳ . مرکز افتا: مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست جمهوری.

۴,۳ دریافت‌کننده خدمات: دستگاه‌های اجرایی متقاضی دریافت خدمات (مشمولین ماده «۲۲۲» و بند «الف» ماده «۲۳۱» قانون برنامه پنجم توسعه جمهوری اسلامی ایران)

۵,۳ پروانه فعالیت: حق اعطاشده توسط سازمان و مرکز افتا به متقاضی احراز صلاحیت شده برای ارائه خدمات افتا.

۶,۳ متقاضی: شخص حقوقی درخواست‌کننده پروانه فعالیت.

۷٫۳ دارنده پروانه فعالیت: شخص حقوقی که با دریافت پروانه فعالیت از سازمان اقدام به فعالیت در چارچوب خدمات موضوع این آیین‌نامه می‌نماید.

۸٫۳ مدت اعتبار: مدت‌زمانی که دارنده پروانه فعالیت می‌تواند در چارچوب پروانه، فعالیت نماید.

۹٫۳ تعهدنامه حفظ کیفیت و محرمانگی: سندی است حاوی کلیه تعهدات، الزامات و ضوابط ارائه خدمات که دارنده پروانه فعالیت مقید به رعایت کلیه مفاد آن است و در صورت احراز شرایط دریافت پروانه فعالیت، قبل از صدور پروانه، توسط متقاضی ارائه داده می شود.

۱۰٫۳ موافقت‌نامه سطح خدمات (SLA): موافقت‌نامه کتبی بین دارنده پروانه فعالیت و دریافت‌کننده خدمات است که بر اساس آن کیفیت سطح خدمات قابل‌ارائه، شاخص و روش‌های اندازه‌گیری و ضمانت‌های اجرایی آن تعیین می‌شود.

۱۱٫۳ تعهدنامه منع افشای اطلاعات (NDA): پیمان کتبی بین دارنده پروانه فعالیت و دریافت‌کننده خدمات که بر اساس آن طرفین متعهد می‌شوند تا اطلاعات محرمانه و اختصاصی یکدیگر را که در حین و بعد از اجرای کار در اختیار طرف مقابل می‌گذارند، افشاء نکنند.

۱۲٫۳ کارشناس ارائه خدمت: به کارکنانی از متقاضی گفته می‌شود که در زمینه ارائه خدمات قلمرو این آئین‌نامه فعالیت داشته باشد.

۴. الزامات عمومی متقاضی و دارنده پروانه فعالیت

۱٫۴ متقاضی می‌بایست شرکتی باشد که ۱۰۰٪ سهام و یا سرمایه آن متعلق به اتباع ایرانی و بر اساس قانون تجارت و با مدیریت ایرانی اداره شود.

۲٫۴ کلیه سهامداران (حقیقی و حقوقی)، مدیران، کارشناسان ارائه خدمت متقاضی باید تابعیت ایرانی داشته باشند (داشتن تابعیت کشوری دیگر و یا تابعیت دوگانه از سوی آن‌ها باعث نقض این بند می‌شود).

۳٫۴ متقاضی می‌بایست در ارزیابی فنی و اعتباری شرایط لازم هر خدمت را اخذ نماید. شرایط و روش ارزیابی هر خدمت (نامبرده شده در پیوست یک) در فرم‌های مرتبط در سایت سازمان بیان شده است.

۴,۴ موضوع فعالیت شرکت متقاضی اخذ پروانه باید پوشش دهنده خدمات بیان شده در این آیین‌نامه (پیوست یک) باشد.

۵,۴ متقاضی علاوه بر الزامات این آئین‌نامه، ملزم به رعایت کلیه سیاست‌های ابلاغی دریافت‌کننده خدمات و سیاست‌های بالادستی و دستورالعمل‌های ابلاغی مرکز افتا می‌باشد.

۶,۴ نشانی دفتر اصلی متقاضی مندرج در آخرین تغییر آن در روزنامه رسمی به‌عنوان نشانی مرجع برای کلیه ابلاغ‌ها و مکاتبات رسمی ملاک عمل بوده و دارنده پروانه فعالیت موظف است در صورت جابجایی محل فعالیت، شامل دفتر اصلی یا شعب، مراتب را حداکثر ۱۵ روز بعد از جابجایی به‌صورت مکتوب به سازمان ابلاغ نماید.

۷,۴ اعمال هرگونه تغییر در مفاد پروانه فعالیت، مستلزم ارائه اصل پروانه فعالیت به سازمان و صدور پروانه فعالیت جدید می‌باشد.

۸,۴ در صورت تصمیم به توقف فعالیت، دارنده پروانه فعالیت موظف است مراتب را به صورت مکتوب حداکثر ظرف مدت ۱۵ روز به سازمان اعلام نماید، بدیهی است توقف فعالیت منوط به رعایت کامل بندهای موافقت‌نامه سطح خدمات (SLA) منعقده با مشتریان تا زمان اتمام مدت اعتبار موافقت‌نامه سطح خدمات است.

۹,۴ دارنده پروانه فعالیت باید کلیه تمهیدات لازم به‌منظور ایجاد زمینه انجام وظایف قانونی نظارتی مراجع ذیصلاح در محل خود را در تمام طول مدت اعتبار پروانه فعالیت به‌صورت حضور در محل و یا اعمال از راه دور در چارچوب قوانین این آئین‌نامه فراهم نماید.

۱۰,۴ دارنده پروانه فعالیت موظف است از کلیه کارشناسان ارائه‌دهنده خدمات حوزه این آئین‌نامه، تعهدنامه عدم افشای اطلاعات (NDA) دریافت نماید.

۱۱,۴ دارنده پروانه فعالیت موظف است تا در قراردادهای موضوع این آئین‌نامه، تعهدنامه‌ی عدم افشای اطلاعات (NDA) را امضا نماید. همچنین در قراردادهای موضوع این آئین‌نامه، قید گردد که دارنده پروانه فعالیت مسئولیت دریافت تعهدنامه‌ی عدم افشای اطلاعات از کلیه نیروهای خود را دارد.

۱۲,۴ تنها کارشناسانی از شرکت متقاضی قادر به ارائه خدمات موضوع این آئین نامه خواهند بود که پس از معرفی توسط شرکت متقاضی، در فرایند ارزیابی تائید شوند. لازم به ذکر است نام کارشناسان تائید شده در پیوست پروانه فعالیت اعلام خواهد شد.

۱۳,۴ دارنده گواهی متعهد است نسبت به ارسال درخواست مجوز بکارگیری کارکنان جدید در حوزه خدمات موضوع گواهی اقدام نماید.کارکنان مذکور حق هیچگونه فعالیتی در حوزه خدمات موضوع گواهی را تا قبل از صدور مجوز از سوی مرکز صدور گواهی نخواهد داشت.

۱۴,۴ دارنده پروانه فعالیت موظف است در اجرای قراردادهای ذیل این آیین‌نامه، از کارشناسان ارائه خدماتی استفاده نماید که از کارکنان آن شرکت باشد و نام آن‌ها در لیست کارشناسان مجاز به ارائه خدمت در پیوست پروانه فعالیت آمده باشد.

۱۵,۴ دارنده پروانه فعالیت ملزم به رعایت تعهدات مندرج در «تعهدنامه حفظ کیفیت و محرمانگی» است.

۵. الزامات فنی متقاضی و دارنده پروانه فعالیت

۱,۵ دارنده پروانه فعالیت خدمات، مکلف است خدمات موضوع پروانه فعالیت را باکیفیت مطلوب و بر اساس موافقت‌نامه سطح خدمات (SLA) به دریافت‌کننده خدمات ارائه نماید.

۶. روال درخواست پروانه فعالیت

۶,۱ روال درخواست پروانه فعالیت به شرح زیر می‌باشد:

- مراجعه به سایت سازمان (http://nama.ito.gov.ir)-درخواست دریافت پروانه
- دریافت فرم‌ها و اسناد راهنما با توجه به پروانه فعالیت مورد درخواست
- تکمیل فرم‌های موردنظر مطابق با راهنماهای مربوطه به همراه مدارک پشتیبان
- حضور نماینده شرکت متقاضی به همراه مدارک تکمیل‌شده در سازمان یا ادارات کل فناوری اطلاعات استان‌های نامبرده شده در سایت سازمان

- ارائه معرفی‌نامه، ممهور به مهر شرکت و امضای مدیرعامل
- ارائه مدارک فنی (دو نسخه لوح فشرده) و اعتباری (یک لوح فشرده به انضمام یک نسخه پرینت ممهور به مهر شرکت و امضای کارشناس)

۷. اسناد و مدارک لازم

۷,۱ اسناد و مدارک موردنیاز برای درخواست پروانه فعالیت شامل اسناد و مدارک ارزیابی فنی و اعتباری می‌باشد که برای هر یک از خدمات مندرج در «پیوست یک»، به‌صورت جداگانه در سایت سازمان اعلام و قابل دریافت می‌باشند. اسناد عمومی موردنیاز برای درخواست پروانه فعالیت به شرح زیر است:

- نامه درخواست تقاضای پروانه
- روزنامه‌ی رسمی نشان‌دهنده‌ی آخرین تغییرات مدیریت و یا سهام‌داران (با مهر و امضا)
- لیست بیمه سه‌ماهه منتهی به تاریخ درخواست پروانه فعالیت به همراه قبض پرداخت و قرارداد کلیه کارشناسان مرتبط با خدمات حوزه‌ی پروانه فعالیت
- فرم‌های ارزیابی تکمیل‌شده به همراه مدارک پشتیبان
- تعهدنامه‌های عدم افشای اطلاعات کلیه کارشناسان ارائه خدمت

۷,۲ تنها مدارک و فرم‌های تکمیل‌شده‌ای معتبر می‌باشند و مورد ارزیابی قرار می‌گیرند که توسط صاحبان امضا مجاز شرکت، مهر و امضا شده باشند.

۷,۳ هنگام ارزیابی در صورت لزوم، پس از هماهنگی از محل شرکت یا موسسه متقاضی بازدید به عمل‌آورده می‌شود و آزمون تخصصی برگزار خواهد شد.

۸. صدور پروانه فعالیت

۸,۱ در صورت کسب صلاحیت‌های لازم، مراتب به متقاضی اعلام می‌گردد و پس از امضا و دریافت «تعهد نامه حفظ کیفیت و محرمانگی»، پروانه فعالیت در حوزه مورد درخواست توسط سازمان صادر می‌گردد.

۸,۲ مدت اعتبار پروانه فعالیت در گواهی قید می‌شود.

۸,۳ اطلاعات دارندگان پروانه فعالیت بر روی سایت سازمان منتشر و به‌روز رسانی می‌گردد.

۹. تمدید، تعلیق، ابطال و تغییر پروانه فعالیت

۹,۱ در صورت وقوع تخلف از مفاد این آیین نامه و یا «تعهدنامه حفظ کیفیت و محرمانگی» توسط دارنده پروانه فعالیت، پس از احراز تخلف، با توجه به نوع تخلف صورت گرفته، پروانه فعالیت مذکور به مدت معین تعلیق یا برای همیشه ابطال شده و موارد به اطلاع متقاضی رسیده و از طرق مقتضی اعلام خواهد شد.

۹,۲ اعتبار پروانه منوط به وجود نام شرکت در لیست شرکت‌های دارای پروانه فعالیت در سایت سازمان است و در صورت تعلیق و یا ابطال پروانه فعالیت، ضمن حذف شدن نام شرکت از لیست مذکور، پروانه فعالیت نیز فاقد اعتبار خواهد شد.

۹,۳ فرایند تمدید پروانه فعالیت با در نظر گرفتن مدارک و مستندات مورد نیاز جهت تمدید با همان روش اجرایی صدور پروانه انجام می‌گردد.

۹,۴ دارنده پروانه فعالیت باید دو ماه قبل از اتمام اعتبار پروانه فعالیت نسبت به ارائه درخواست تمدید به سازمان، اقدام نماید.

۹,۵ پس از بررسی و ارزیابی‌های لازم درخواست دارنده پروانه فعالیت و تکمیل مدارک مورد نیاز توسط وی، تمدید مجوز از سوی سازمان صورت خواهد پذیرفت.

۹,۶ تغییر در مدارک حقوقی و نیز ترکیب اعضای حقیقی و حقوقی تاثیرگذار در فعالیت‌های موضوع این آئین‌نامه در سمت دارنده پروانه فعالیت، باید با ارائه مستندات کامل، به سازمان منعکس شده و اعتبار پروانه منوط به ارزیابی مجدد است.

۹,۷ اعمال هرگونه تغییرات در مفاد پروانه فعالیت مستلزم ارائه اصل پروانه فعالیت پیشین به سازمان و صدور پروانه فعالیت جدید می‌باشد.

۱۰. رسیدگی به تخلفات و شکایات

۱۰,۱ مرجع رسیدگی به شکایات و داوری در حل اختلافات میان دارندگان پروانه‌ی فعالیت، سازمان با همکاری مرکز افتا می‌باشد.

۱۰,۲ مرجع رسیدگی به شکایات و داوری در حل اختلافات میان دارنده‌ی پروانه فعالیت و دریافت کنندگان خدمات، مرکز افتا می‌باشد.

۱۱. ضوابط مالی

۱۱,۱ متقاضی موظف است پس از تعیین و اعلام هزینه صدور پروانه فعالیت، مطابق با تعرفه تایید شده از سوی مراجع ذی‌صلاح، نسبت به پرداخت آن اقدام نماید.

۱۲. به‌روز رسانی

۱۲,۱ سازمان در اقدامی مشترک با مرکز افتا این آئین‌نامه را در دوره‌های سه‌ساله مورد بررسی قرار می‌دهد و در صورت نیاز به بهینه‌سازی مطابق شرایط روز اقدام می‌نمایند. برحسب ضرورت و تایید مشترک مدیران ارشد سازمان و مرکز افتا، این فرایند می‌تواند درزمانی کمتر به مورد اجرا درآید.

پیوست یک: انواع خدمات امنیتی فناوری اطلاعات

در این آیین‌نامه خدمات امنیتی فناوری اطلاعات بر اساس دسته‌بندی کلان خدمات به چهار نوع خدمت تقسیم‌بندی شده‌اند که عبارتند از:

۱. خدمات مدیریتی افتا
۲. خدمات عملیاتی افتا
۳. خدمات فنی افتا
۴. خدمات آموزشی افتا

هریک از این حوزه‌ها دربرگیرنده‌ی مجموعه‌ای از گرایش‌ها هستند که در ادامه هریک از آنها تشریح می‌گردد.

لازم به ذکر است که برای برخی خدمات به صورت مقطعی و با ظرفیت محدود امکان درخواست پروانه فعالیت وجود خواهد داشت.

خدمات مدیریتی افتا

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 است. لذا ارائه خدمات کلان ذیل در این حوزه قرار می‌گیرد:

- مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات
- ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات
- طرح ریزی معماری و زیرساخت امنیت
- ارائه مشاوره حقوقی در زمینه افتا
- خدمات بیمه افتا

قابلیت‌ها و مهارت‌های مربوط به متقاضیان هریک از گرایش‌های مذکور در ادامه آمده است.

پ ۱,۱ مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات[۱]

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمت عبارتند از:

- توانایی تعیین سطح امنیتی مناسب برای محافظت از سازوکار و دارائی‌های سازمان‌ها
- توانایی تحلیل و مدیریت ریسک
- توانایی تدوین خط‌مشی، فرایندها و راهنماهای امنیتی
- تسلط بر استانداردهای مدیریت امنیت اطلاعات و مدیریت فناوری اطلاعات و تدوام کسب و کار و ITIL و COBIT
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات
- توانمندی‌های عمومی مشاوره

پ ۲,۱ ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات

تذکر: متقاضیان ارائه این خدمت نمی‌توانند در گرایش مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات فعالیت نمایند.

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمت عبارتند از:

- مطابقت با چک‌لیست الزامات ممیزی و صدور گواهینامه
- مطابقت با استانداردهای الزامات مراکز گواهی در حوزه سیستم‌های مدیریتی فتا و افتا
- توانایی توسعه و پشتیبانی از یک طرح امنیتی برای هر سیستم و دارائی‌های تحت کنترل سازمان
- توانایی تحلیل و مدیریت ریسک
- تسلط بر خط‌مشی، فرایندها و راهنماهای امنیتی
- تسلط بر استانداردهای مدیریت امنیت اطلاعات، مدیریت فناوری اطلاعات و تدوام کسب و کار
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات

[۱] مانند 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 رخداد (IM) و مانند آن

پ ۳,۱ طرح ریزی معماری و زیرساخت امنیت

دارنده این پروانه فعالیت می‌تواند به عنوان مجری «طرح امن‌سازی زیرساخت‌های حیاتی در مقابل حملات الکترونیکی» فعالیت نماید. شرط لازم برای درخواست این پروانه فعالیت، داشتن پروانه فعالیت «مشاوره و استقرار استانداردهای مدیریت امنیت اطلاعات و ارتباطات» و نیز داشتن حداقل دو پروانه فعالیت از چهار گرایش زیر باشد:

- آزمون و ارزیابی امنیتی
- پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد
- امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها
- راهبری مرکز عملیات امنیت و تیم پاسخگویی به رخداد

براین اساس متقاضیان دریافت این پروانه فعالیت باید مهارت‌ها و قابلیت‌های مطرح شده در گرایش‌های مذکور را دارا باشند.

پ ۴,۱ ارائه مشاوره حقوقی در زمینه افتا

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمت عبارتند از:

- آشنایی با قوانین و مقررات پی‌جویی وکشف جرایم سایبری
- آشنایی با قوانین حوزه فناوری اطلاعات در ایران
- آشنایی با نحوه پی‌جویی و کشف جرایم سایبری
- آشنایی با اصول عملکرد سیستم‌های پیشگیری از افشای اطلاعات (برای مثال در مهندسی اجتماعی)

پ ۵,۱ خدمات بیمه افتا

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمت عبارتند از:

- آشنایی با ریسک‌های فاوا قابل ارزیابی و بیمه‌پذیر
- توانایی در عرضه بیمه افتا

- دارا بودن الزامات قانونی تاسیس شرکت بیمه مطابق با آیین نامه شماره ۷۱ بیمه مرکزی جمهوری اسلامی ایران

خدمات عملیاتی افتا

خدمات عملیاتی افتا، بیشتر بر مهارت‌های خاص و یا فنی پرسنل برای پیاده‌سازی و یا حصول اطمینان از عملکرد مناسب کنترل‌های پیاده‌سازی شده تاکید دارد. لذا ارائه خدمات کلان ذیل در این حوزه قرار می‌گیرد:

- آزمون و ارزیابی امنیتی
- پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد
- پیاده‌سازی امنیت فیزیکی و محیط پیرامونی
- امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها
- راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد

در ادامه، مفهوم هریک از خدمات مذکور و دامنه شمول فعالیت‌های هر حوزه مطرح شده‌است. همچنین عمده مهارت‌ها و قابلیت‌هایی که برای متقاضیان هریک از این گرایش‌ها متصور است نیز در این بخش بیان می‌گردد.

پ ۱,۲ آزمون و ارزیابی امنیتی

خدمت آزمون و ارزیابی امنیتی شامل کلیه خدمات ارزیابی امنیتی نرم‌افزار، تجهیزات، سرویس‌ها و سامانه‌ها، آزمون نفوذپذیری و آزمون آسیب‌پذیری می‌باشد.

خدمات قابل ارائه در این گرایش عبارتند از:

- بررسی صحت سیستم
- پویش سیستم و شبکه
- ارزیابی آسیب‌پذیری سامانه، تجهیزات و سرویس ها
- آزمون نفوذپذیری سامانه، تجهیزات و سرویس ها
- ارزیابی امنیتی سامانه، تجهیزات و سرویس ها
- فارنزیک سامانه، تجهیزات و سرویس ها

مهارت‌ها و قابلیت‌های لازم برای ارائه «خدمات آزمون و ارزیابی امنیتی» عبارتند از:

- آگاهی، دانش و تسلط کافی بر سیستم‌عامل‌ها، شبکه و پروتکل‌های شبکه، پایگاه داده و برنامه‌های کاربردی
- آگاهی، دانش و تسلط کافی بر سرویس‌های شبکه
- آشنایی با بدافزارها، حملات و آسیب‌پذیری‌ها و توانایی ارائه راه‌حل برای کاهش اثر/جلوگیری از آن‌ها
- آگاهی از مفاهیم مهندسی معکوس
- توانایی تحلیل و کشف آسیب‌پذیری
- توانایی ارزیابی و مدیریت آسیب‌پذیری
- آگاهی از مفاهیم فارنزیک سیستم
- آشنایی و توانایی کار با ابزارهای آزمون
- آشنایی و تسلط بر انواع متدلوژی‌های آزمون
- آگاهی در مورد استانداردهای مدیریت امنیت اطلاعات

پ ۲,۲ پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد

خدمات مرتبط با پیاده‌سازی مرکز عملیات امنیت و یا تیم پاسخ به رخداد به خدماتی اطلاق می‌شود که وظیفه راه‌اندازی و پشتیبانی از تجهیزات و سامانه‌های مرتبط با مرکز عملیات امنیت و تیم پاسخ به رخداد 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 و یا تیم پاسخ به رخداد در محیط کارفرما مورداستفاده قرار می‌گیرد. در واقع پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد شامل سه بعد فرآیندها (رویه‌ها)، تجهیزات و آموزش نیروی انسانی می‌باشد.

شرکت‌های ارائه‌دهنده این نوع خدمت لازمست توانمندی انجام فعالیت‌های زیر را داشته باشند:

- طراحی و راه‌اندازی مرکز عملیات امنیت
- طراحی و پیاده‌سازی رویه‌های مدیریت رخداد
- توسعه برنامه مدیریت رخداد
- توسعه و پشتیبانی از پروفایل‌های پیکربندی سیستم
- فراهم‌سازی قابلیت فارنزیک
- آزمون و به‌روزرسانی رویه‌های مدیریت رخداد

- تهیه طرح تداوم کسب‌وکار
- تهیه طرح بازیابی از فاجعه
- مشاوره در هر یک از خدمات ذکر شده

مهارت‌های لازم برای ارائه این خدمت عبارتند از:

- توانایی برنامه‌ریزی توسعه و مدیریت رخداد
- تسلط بر انواع حملات شبکه بی‌سیم و باسیم
- آگاهی از مفاهیم فارنزیک سیستم و شبکه
- توانایی به‌روزرسانی و مدیریت رویه‌های مدیریت رخداد (با توسعه ابزارها و تکنیک‌ها)
- تسلط بر مفاهیم و معماری شبکه
- تسلط در زمینه امنیت شبکه، سیستم‌عامل، پایگاه داده و برنامه‌های کاربردی
- تسلط بر پیکربندی تجهیزات شبکه
- توانایی پیکربندی امن تجهیزات نرم‌افزاری و سخت‌افزاری

پ ۳,۲ پیاده‌سازی امنیت فیزیکی و محیط پیرامونی

این گرایش شامل طراحی، نصب، پیکربندی و پشیبانی از راه‌حل‌های ایجاد امنیت فیزیکی و محیط پیرامونی است.
شرکت‌های ارائه‌دهنده این نوع خدمت لازمست توانمندی انجام فعالیت‌های زیر را داشته باشند:

- امن‌سازی و مقاوم‌سازی امن اتاق سرور و مراکز داده
- 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
- طراحی و پیاده‌سازی امنیت محیط پیرامونی

مهارت‌های لازم برای ارائه این خدمت عبارتند از:

- تسلط بر مکانیزم‌های فیزیکی کنترل دسترسی
- تسلط بر ایمن‌سازی محیطی برای حوزه فناوری اطلاعات
- تسلط بر مکانیزم‌ها و راه حل‌های امنیت محیط پیرامونی

- آشنایی با تجهیزات امنیت محیط پیرامونی
- تسلط بر راه‌حل‌های تامین مطمئن برق
- ارزیابی امنیت فیزیکی

پ ۴,۲ امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها

ارائه دهنده‌ی این نوع گرایش نسبت به امن‌سازی و مقاوم‌سازی شبکه، سیستم، سرویس‌ها، تجهیزات نرم‌افزاری و سخت‌افزاری برای مقابله با بدافزارها، دسترسی‌های غیرمجاز و نفوذگران در محیط کارفرما اقدام می‌نماید. مقاوم‌سازی سامانه‌ها و همچنین پیاده‌سازی طرح‌های تداوم کسب‌وکار در حوزه فناوری اطلاعات و طراحی و پیاده-سازی شبکه امن در رده این گرایش قرار می‌گیرند.

شرکت‌های ارائه‌دهنده این نوع خدمت لازمست توانمندی انجام فعالیت‌های زیر را داشته باشند:

- ارائه‌ی معماری امن شبکه
- ارائه‌ی راه‌حل و پیاده‌سازی چارچوب برای تداوم کسب و کار امنیتی
- امن‌سازی و مقاوم‌سازی برنامه‌های کاربردی، پایگاه داده‌ها، سرویس‌ها و سیستم‌عامل
- توسعه‌ی برنامه‌ی بازیابی و پشتیبان‌گیری امن داده‌ها
- امن‌سازی و مقاوم‌سازی زیرساخت‌ها و استفاده از رمزنگاری و پروتکل‌های ارتباطی امن
- مشاوره در مورد هر یک از خدمات موارد ذکر شده

مهارت‌های لازم برای ارائه این خدمت عبارتند از:

- تسلط بر مفاهیم و معماری شبکه
- تسلط بر راهبری و پیکربندی تجهیزات شبکه
- تسلط بر امن‌سازی و مقاوم‌سازی سیستم‌ها، سرورها و شبکه
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- تسلط بر راه‌حل‌های مرتبط با تداوم کسب‌وکار در فناوری اطلاعات
- تسلط بر مجازی‌سازی و رایانش ابری
- ارزیابی و مدیریت ریسک و آسیب‌پذیری‌ها
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- آگاهی از استانداردهای مدیریت فناوری اطلاعات و مدیریت امنیت فناوری اطلاعات

پ ۵,۲ راهبری مرکز عملیات امنیت و تیم پاسخ به رخداد

خدمات مرتبط با راهبری مرکز عملیات امنیت و یا تیم پاسخ به رخداد به خدماتی اطلاق می‌شود که به منظور راهبری امنیتی، مدیریت رخدادهای امنیتی و حفظ اطلاعات، پایش وقایع امنیتی، شناسایی حوادث امنیتی و رسیدگی به موقع به آن‌ها در محیط کارفرما مورد استفاده قرار می‌گیرد. این خدمات می‌توانند به‌صورت خدمات امنیتی مدیریت شده نیز ارائه گردند.

شرکت‌های ارائه‌دهنده این نوع خدمت لازمست توانمندی انجام فعالیت‌های زیر را داشته باشند:

- راهبری امن مرکز عملیات امنیت
- راهبری امن رویه‌های مدیریت رخداد
- انجام اقدامات اولیه فارنزیک
- اجرای اقدامات اصلاحی اولیه

مهارت‌های لازم برای ارائه این خدمت عبارتند از:

- آشنایی با ابزارهای پایش ترافیک و رکوردهای ثبت شده
- تسلط کافی بر انواع حملات شبکه بی‌سیم و باسیم
- آشنایی با اقدامات فارنزیک سیستم و شبکه
- توانایی پشتیبان‌گیری و بازیابی داده‌ها
- توانایی به‌روزرسانی و مدیریت رویه‌های مدیریت رخداد (راهبری رویه‌ها)
- تسلط کافی بر مفاهیم و معماری شبکه
- تسلط کافی در زمینه امنیت شبکه، سیستم‌عامل، پایگاه داده و برنامه‌های سیستمی
- تسلط فنی بر استفاده از تجهیزات شبکه

پ.۱خدمات فنی افتا

خدمات فنی افتا، شامل پیکربندی امن و پشتیبانی امنیتی محصول فتا می‌باشد و متقاضیان در این حوزه می‌بایست برای محصول مورد نظر گواهی ارزیابی امنیتی دریافت کرده باشند. شایان ذکر است با توجه به درخواست متقاضی، عنوان محصول مورد تایید در پروانه فعالیت صادر شده در این گرایش ذکر می‌شود.

پ.۱,۳ نصب و پشتیبانی محصولات فتا:

این گرایش خدمات شامل خدمات نصب، راه‌اندازی، پیکربندی، به‌روزرسانی، پشتیبانی و آزمایش و تحویل هر نوع خدمات فنی مرتبط با محصولات فتا می‌شود.

مهارت‌های لازم برای ارائه این خدمت عبارتند از:

- تسلط فنی متقاضی بر پیکربندی امن محصول
- تسلط فنی متقاضی در پشتیبانی امن محصول
- تسلط فنی متقاضی بر روش‌های مختلف استفاده از محصول
- صلاحیت فرایندی و اعتباری پشتیبانی از محصول (تعامل متقاضی با شرکت تولیدکننده محصول)

خدمات آموزشی افتا

این حوزه خدمات شامل ارائه آموزش کلیه دوره‌های امنیتی در سطوح و موضوعات مختلف به متقاضیان است.

تذکر: دامنه این حوزه مربوط به آموزش‌هایی می‌باشد که منجر به دریافت گواهینامه‌های ملی و بین‌المللی در زمینه دوره‌های آموزشی امنیت اطلاعات و ارتباطات گردد.

پ.۱,۴ برگزاری دوره‌های آموزشی افتا

گرایش این خدمت شامل برگزاری دوره های آموزش امنیتی در سطوح و موضوعات مختلف می‌باشد. شایان ذکر است با توجه به درخواست متقاضی، عنوان آموزش مورد تایید، در گواهی صادر شده در این گرایش ذکر می‌شود.

علاوه بر اینکه شرکت متقاضی باید شرایط، فضا و تجهیزات مناسب با دوره‌های آموزشی را فراهم نماید. لازم است تا مدرس دوره نیز مهارت و توانایی لازم برای برگزاری آن دوره را داشته باشد.

مهارت‌ها و قابلیت‌های لازم برای مدرسین در ارائه این خدمت عبارتند از:

- آشنایی با مدیریت کیفیت خدمات آموزش
- آشنایی با مدیریت موثر آموزش
- آشنایی با الزامات استانداردهای آموزش و مدیریت امنیت
- توانایی ارائه محصولات کمک‌آموزشی و راه‌اندازی کارگاه آموزشی و برگزاری سمینارهای تخصصی

- تسلط فنی بر دوره‌های آموزشی از قبیل امنیت سیستم‌عامل، شبکه، پایگاه داده، برنامه‌های کاربردی، بدافزار، استانداردهای امنیتی
- آگاهی از مستندات NIST SP 800-16 و NIST SP 800-50 و دیگر مستندات و استانداردهای مربوطه
- داشتن مجوز استانداردی مبنی بر ارائه خدمات آموزش