## موضوع: راهنمای تکمیل فایل های درخواست مجوز خدمات

### ۱- مقدمه

در طرح ساماندهی شرکت های ارائه کننده خدمات افتا، این خدمات به چهار حوزه کلان تقسیم بندی شده‌اند که عبارتند از :

- خدمات مدیریت امنیت
- خدمات عملیاتی امنیتی
- خدمات فنی امنیتی
- خدمات آموزش امنیت

هر یک از این حوزه‌ها نیز دارای گرایش های مختلف خدمات هستند که عبارتند از:

- خدمات مدیریت افتا
  - گرایش مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات
  - گرایش ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات
  - گرایش طرح ریزی معماری و زیرساخت امنیت
  - گرایش ارائه مشاوره حقوقی در زمینه امنیت فناوری اطلاعات
  - گرایش خدمات بیمه امنیت اطلاعات و ارتباطات
- خدمات عملیاتی افتا
  - آزمون و ارزیابی امنیتی
  - پیاده‌سازی مرکز عملیات امنیت و یا مرکز پاسخ به رخداد
  - راهبری مرکز عملیات امنیت و یا تیم پاسخ به رخداد
  - امن‌سازی و پشتیبانی امنیتی سامانه‌ها، زیرساخت‌ها و سرویس‌ها
  - پیاده‌سازی امنیت فیزیکی و محیط پیرامونی
  - راهبری امنیت فیزیکی و محیط پیرامونی
- خدمات فنی افتا
  - گرایش نصب و پشتیبانی تجهیزات امنیتی سخت‌افزاری و نرم‌افزاری
- خدمات آموزش افتا
  - گرایش آموزشی این حوزه در متن گواهی قید می‌گردد.

شرکت‌های متقاضی فعال در دسته بندی انجام شده می‌توانند بر اساس حوزه های خدمات خود اقدام به تکمیل فرم های مربوطه و درخواست مجوز نمایند.

فایل‌های ارزیابی فنی درخواست گواهی شامل دو فایل می‌باشد که در قالب InfoPath در سایت قرار دارند. فایل Company.xsn که شامل اطلاعات کلی در مورد شرکت ارائه کننده خدمات افتا است و فایل Service.xsn که بیانگر قابلیت‌های شرکت در ارائه هر خدمت است. هر شرکت برای هر حوزه خدمت اقدام به تکمیل یک فایل Company.xsn و یک فایل Servic.xsn می نماید.

علاوه بر فایل‌های ارزیابی فنی، شرکت باید مطابق راهنمای تکمیل فرم‌های ارزیابی اعتباری، اقدام به تکمیل و به سازمان ارسال نماید.

برای فرم‌های ارزیابی فنی نیز، پس از تکمیل فایل‌های مربوطه، شرکت متقاضی باید دونسخه –دو لوح فشرده- از تمامی فایل‌های مربوط به ارزیابی فنی، Company.xsn و Service.xsn را -که برای هر حوزه خدمت به‌طور جداگانه تکمیل شده است- به همراه یک نسخه از فرم سهام‌داران که در پوشه اعتباری قرار دارد، را به سازمان تحویل نماید.

## ۲- شرح خدمات افتا

در این بخش هر یک از حوزه‌ها و گرایش های خدمات به تفصیل بر اساس ماهیت خدمت و مهارت های فنی لازم برای آن خدمت شرح داده می شوند.

### ۲-۱- خدمات مدیریت افتا

خدمات مدیریت افتا، خدماتی از جنس طراحی‌های کلان و ساختاری، طرح‌ریزی، برنامه‌ریزی، بهبود و ساماندهی، سنجش و پیشگیری مخاطرات امنیتی در سازمان‌ها و یا نظام‌های فناوری اطلاعات و ارتباطات است. لذا ارائه گرایش‌های خدمات کلان ذیل در دسته مدیریت امنیت قرار می‌گیرد.

- مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات[۱]

مهارت‌ها و قابلیت‌های لازم برای ارائه خدمات در این گرایش عبارتند از:

- توانایی تعیین سطح امنیتی مناسب برای محافظت از سازوکار و دارائی‌های سازمان‌ها
- توانایی تحلیل و مدیریت ریسک
- تسلط کافی بر خط‌مشی، فرایند و راهنماهای امنیتی

[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

- آگاهی کافی در مورد استانداردهای سری ISO 27000 و مستندات NIST SP 800-30-800-12 NIST SP و دیگر استانداردها و مستندات مرتبط با مدیریت امنیت اطلاعات
- آشنایی با استانداردهای ITIL و COBIT
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات
- توانمندی‌های عمومی مشاور

- ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات

مهارت‌ها و قابلیت‌های لازم برای ارائه خدمات در این گرایش عبارتند از:

- مطابق با چک‌لیست الزامات ممیزی و صدور گواهینامه
- تطابق با استانداردهای الزامات مراکز گواهی از قبیل ISO 17021 و ISO 27006
- توانایی توسعه و پشتیبانی از یک طرح امنیتی برای هر سیستم و دارائی‌های تحت کنترل سازمان
- توانایی تحلیل و مدیریت ریسک
- تسلط کافی بر خط‌مشی، فرایند و راهنماهای امنیتی
- آگاهی کافی در مورد استانداردهای سری ISO 27000 و مستندات NIST SP 800-30-800-12 NIST SP و دیگر استانداردها و مستندات مرتبط با مدیریت امنیت اطلاعات
- آشنایی با استانداردهای ITILو COBIT
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات

- طرح ریزی معماری و زیرساخت امنیت

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارتند از:

- توانایی تعیین سطح امنیتی مناسب برای محافظت از سازوکار و دارائی‌های سازمان‌ها
- توانایی توسعه و پشتیبانی از یک طرح امنیتی برای هر سیستم و دارائی‌های تحت کنترل سازمان
- توانایی تحلیل و مدیریت ریسک

- تسلط کافی بر خط‌مشی، فرایند و راهنماهای امنیتی
- آگاهی کافی در مورد استانداردهای سری ISO 27000 و مستندات NIST SP 800-30-800-12 NIST SP و دیگر استانداردها و مستندات مرتبط با مدیریت امنیت اطلاعات
- آشنایی با استانداردهای ITIL و COBIT
- آشنایی با استانداردهای ارزیابی امنیتی
- آشنایی با مدل‌های بلوغ امنیت اطلاعات

- ارائه مشاوره حقوقی در زمینه امنیت فناوری اطلاعات

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارتند از:

- آشنایی با قوانین و مقررات پی جویی وکشف جرایم سایبری
- آشنایی با قوانین حوزه فناوری اطلاعات در ایران
- آشنایی با نحوه پی جویی و کشف جرایم سایبری
- آشنایی با اصول عملکرد سیستم های پیشگیری از افشای اطلاعات (مهندسی اجتماعی)

- خدمات بیمه امنیت اطلاعات و ارتباطات

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات 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

### ۲-۲- خدمات عملیات افتا

خدمات عملیات افتا، خدماتی است که بیشتر بر مهارت‌های خاص و یا فنی پرسنل برای پیاده‌سازی و یا حصول اطمینان از عملکرد مناسب کنترل‌های پیاده‌سازی شده تاکید دارد. لذا گرایش‌های ارائه خدمات ذیل در این دسته قرار می‌گیرد:

- آزمون و ارزیابی امنیتی

خدمات عملیاتی آزمون و ارزیابی امنیتی یکی از گرایش‌های فعالیت شرکت‌های متقاضی دریافت مجوز در دسته «خدمات عملیاتی امنیتی» است که شامل کلیه خدمات ارزیابی امنیتی نرم‌افزار، تجهیزات، سرویس‌ها و سامانه‌ها، تست نفوذ و تست آسیب‌پذیری می‌شود. این گرایش از خدمات عملیاتی شامل ارائه خدماتی به شرح زیر می‌باشد:

- بررسی صحت سیستم
- پویش سیستم و شبکه
- ارزیابی آسیب‌پذیری سامانه، تجهیز و سرویس
- تست نفوذ سامانه، تجهیز و سرویس
- ارزیابی امنیتی سامانه، تجهیز و سرویس
- فارنزیک سامانه، تجهیز و سرویس

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 در مفاهیم مهندسی معکوس
- توانایی تحلیل و کشف آسیب‌پذیری
- توانایی ارزیابی و مدیریت آسیب‌پذیری
- آگاهی از مفاهیم فارنزیک سیستم
- آشنایی و توانایی کار با ابزارهای تست
- آشنایی و تسلط بر انواع متدلوژی‌های تست
- آگاهی در مورد استانداردهای سری ISO 27000 و دیگر استانداردها و مستندات مرتبط با مدیریت امنیت اطلاعات

- <u>پیاده‌سازی/ راهبری مرکز عملیات امنیت و یا تیم پاسخ به رخداد</u>

خدمات مرتبط با تیم پاسخ به رخداد، به خدماتی اطلاق می‌شود که برای مدیریت رخدادهای امنیتی و حفظ اطلاعات و کاهش رخدادهای امنیتی و جلوگیری از بروز تبعات بعدی در سازمان‌ها انجام می‌گردد.

خدمات مرتبط با راه‌اندازی مرکز عملیات امنیت نیز به خدماتی اطلاق می‌شود که برای پایش بلادرنگ وقایع امنیتی، شناسایی حوادث امنیتی و ارائه راهکارهای مقابله با آن‌ها در سازمان مورداستفاده قرار می‌گیرد و شامل سه بعد فرآیندها و رویه‌ها، تجهیزات و نیروی انسانی می‌باشد. شرکت‌های ارائه‌دهنده این نوع خدمات قابلیت انجام فعالیت‌های زیر را دارند:

- طراحی و راه‌اندازی/ راهبری امن مرکز عملیات امنیت
- طراحی و پیاده‌سازی/ راهبری امن رویه‌های مدیریت رخداد
- مشاوره و توسعه برنامه مدیریت رخداد
- مشاوره و توسعه و نگهداری از پروفایل‌های پیکربندی سیستم
- فراهم‌سازی قابلیت فارنزیک
- تست و به‌روزرسانی رویه‌های مدیریت رخداد
- تهیه طرح تداوم کسب‌وکار
- تهیه طرح بازیابی از فاجعه
- مشاوره در هر یک از خدمات گفته‌شده

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارتند از:

- توانایی برنامه‌ریزی توسعه و مدیریت رخداد
- توانایی نظارت و تحلیل بر ترافیک و logها
- تسلط کافی بر انواع حملات شبکه بی‌سیم و سیمی
- آگاهی از مفاهیم فارنزیک سیستم و شبکه
- توانایی بازیابی و پشتیبان‌گیری از داده‌ها
- توانایی به‌روزرسانی و مدیریت رویه‌های مدیریت رخداد
- توانایی اولویت‌بندی رخداد و ارائه راهکار
- تسلط کافی بر مفاهیم و معماری شبکه
- تسلط کافی در زمینه امنیت شبکه، سیستم‌عامل، پایگاه داده و برنامه‌های کاربردی
- تسلط فنی بر استفاده و پیکربندی تجهیزات شبکه
- توانایی پیکربندی امن تجهیزات نرم‌افزاری و سخت‌افزاری

- <u>پیاده‌سازی/ راهبری امنیت فیزیکی و محیط پیرامونی</u>

این دسته خدمت شامل طراحی، نصب، پیکربندی و پشیبانی راه‌حل‌های ایجاد امنیت فیزیکی و محیط پیرامونی است. ازجمله خدمات این دسته می‌توان به موارد زیر اشاره کرد:

- امن سازی/ راهبری امن اتاق سرور و مراکز داده
- طراحی و پیاده‌سازی سامانه‌های اطفای حریق در محیط‌های مرتبط با فناوری اطلاعات
- طراحی و پیاده‌سازی راه‌حل‌های تامین مطمئن برق برای تجهیزات فناوری اطلاعات
- طراحی و پیاده‌سازی سامانه‌های کنترل دسترسی فیزیکی مانند سیستم‌های کنترل ورود/خروج
- طراحی و پیاده‌سازی/ راهبری امن امنیت محیط پیرامونی

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارتند از:

- تسلط فنی بر مکانیزم های فیزیکی کنترل دسترسی
- تسلط فنی بر ایمن‌سازی محیطی برای حوزه فناوری اطلاعات
- تسلط فنی بر مکانیزمها و راه حلهای امنیت محیط پیرامونی
- آشنایی با تجهیزات امنیت محیط پیرامونی
- تسلط فنی بر راه‌حل‌های تامین مطمئن برق

- امن‌سازی و پشتیبانی امنیتی سامانه‌ها، زیرساخت‌ها و سرویس‌ها

این نوع خدمات، به خدماتی اطلاق می‌شود که برای امن‌سازی شبکه و سیستم و سرویس‌ها و تجهیزات نرم‌افزاری و سخت‌افزاری برای مقابله با بدافزارها، دسترسی‌های غیرمجاز و نفوذگران در سازمان بکار گرفته می‌شود. مقاوم‌سازی سامانه‌ها و پیاده‌سازی طرح‌های تداوم کسب‌وکار در حوزه فناوری اطلاعات در این رده خدمات قرار می‌گیرند. طراحی و پیاده‌سازی شبکه امن، نگهداری (راهبری) امنیت در این گرایش قرار می‌گیرد. شرکت‌های ارائه‌کننده این نوع خدمت، مهارت‌ها و قابلیت‌های لازم برای ارائه خدمات زیر را دارا هستند:

- ارائه معماری امن شبکه
- ارائه راه‌حل و پیاده‌سازی چارچوب برای تداوم کسب و کار امنیتی
- امن‌سازی/ راهبری امن برنامه‌های کاربردی، پایگاه داده‌ها و سرویس‌ها و سیستم‌عامل
- توسعه برنامه بازیابی و پشتیبان‌گیری امن داده‌ها
- امن‌سازی/ راهبری امن زیرساخت‌ها و استفاده از رمزنگاری و پروتکل‌های ارتباطی امن
- مشاوره در مورد هر یک از خدمات گفته شده

مهارت‌ها و توانمندی‌های لازم برای ارائه این خدمات عبارتند از:

- تسلط کافی بر مفاهیم و معماری شبکه

- تسلط فنی بر استفاده و پیکربندی تجهیزات شبکه
- تسلط کافی بر امن‌سازی سیستم‌ها، سرورها و شبکه
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- تسلط کافی بر راه‌حل‌های مرتبط با تداوم کسب‌وکار در فناوری اطلاعات
- تسلط کافی بر مجازی‌سازی و رایانش ابری
- ارزیابی و مدیریت ریسک و آسیب‌پذیری‌ها
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- آگاهی از استانداردها و مستندات ITIL وNIST SP 800-32 و NIST SP 800-25 و NIST SP 800-53 و دیگر استانداردها و مستندات مرتبط

## ۲-۳- خدمات فنی افتا

خدمات فنی افتا، به پیاده سازی کنترل‌های امنیتی در سطح یک کامپیوتر اشاره دارد و شامل ارائه خدمت در سطح یک تجهیز است. تا زمانی‌که شرکت‌های متقاضی گواهی خدمت فنی امنیتی برای محصول مورد نظر گواهی ارزیابی امنیتی دریافت نکرده‌باشند امکان درخواست گواهی این گرایش را ندارند.

- گرایش نصب و پشتیبانی تجهیزات امنیتی سخت‌افزاری و نرم‌افزاری

این گرایش خدمات شامل خدمات نصب، راه‌اندازی، پیکربندی، بروزرسانی، پشتیبانی و آزمایش و تحویل و هر نوع خدمات فنی مرتبط با تجهیزات امنیتی سخت افزاری یا نرم افزاری فناوری اطلاعات و ارتباطات می‌شود.

مهارت‌ها و قابلیت‌های لازم برای ارائه این خدمات عبارتند از:

- آشنایی و پیکربندی امن تجهیزات امنیتی مانند IDS, Firewall, SIEM و ...
- تسلط کافی بر مفاهیم و معماری شبکه
- تسلط فنی بر استفاده و پیکربندی تجهیزات شبکه
- تسلط کافی برای ذخیره‌سازی امن
- آشنایی با انواع پروتکل‌های امن و رمزنگاری
- آشنایی با سیستم های رمزنگاری مانند زیرساخت کلید عمومی، کتابخانه های رمزنگاری، سیستم های احراز هویت و ...
- آشنایی با مفاهیم امنیت شبکه، سیستم‌عامل، برنامه‌های کاربردی و پایگاه داده
- توانایی نگهداری و برطرف سازی مشکلات تجهیزات امنیتی
- توانایی تست و ارزیابی صحت عملکرد تجهیزات امنیتی

- توانایی کار با ابزارهای تست تجهیزات امنیتی
- خدمات جانبی مانند بروزرسانی و پشتیبانی فنی
- ارائه مستنداتی نظیر راهنمای استفاده و لیست اجزای تجهیزات ارائه شده
- توانایی همکاری در امور مربوط به جرم شناسی
- توانایی ارائه آموزش به مشتری در صورت نیاز

### ۲-۴- خدمات آموزش افتا

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

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

- گرایش‌های آموزش امنیت

این دسته خدمات شامل ارائه آموزش دوره‌های امنیتی در سطوح و موضوعات مختلف در سازمان می‌باشد (مانند آموزش ISMS).

مهارت‌ها و قابلیت‌های لازم برای مدرسین در ارائه این خدمات 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 گرایش‌های آموزش 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 این گرایش
- داشتن مجوز استانداری مبنی بر ارائه خدمات آموزش
- درج «ارائه خدمات آموزش» در اساسنامه

## ۳- نحوه تکمیل و ارائه مدارک

شرکت‌های متقاضی فعال در دسته‌بندی انجام شده می‌توانند بر اساس حوزه‌های خدمات خود اقدام به تکمیل فرم های مربوطه و درخواست مجوز نمایند.

فایل‌های ارزیابی فنی درخواست گواهی شامل دو فایل می‌باشد که در قالب InfoPath در سایت در پوشه «فایل‌های قابل ارائه به سازمان» قرار دارند. برای تکمیل این فرم ها باید از Microsoft office InfoPath 2013 استفاده شود. فایل Company.xsn که شامل اطلاعات کلی در مورد شرکت ارائه‌کننده خدمات افتا است و فایل Service.xsn که بیانگر قابلیت‌های شرکت در ارائه هر خدمت است. هر شرکت تنها یک‌بار اقدام به تکمیل فایل Company.xsn می‌نماید، اما برای هر گرایش خدمت اقدام به تکمیل یک فایل مجزا برای آن گرایش خدمت می‌نماید. به عنوان نمونه شرکتی که ارائه کننده خدمات عملیاتی امنیتی در دو گرایش آزمون و ارزیابی امنیتی و نیز امن‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها است، یک فایل تکمیل شده Company.xsn با تغییر کلمه Company به نام شرکت خود و دو فایل تکمیل شده service.xsn به نام‌های Test.xsn و Securing.xsn را ارسال می‌نماید. نام حوزه از «جدول شماره ۱» انتخاب شود.

**توجه : علاوه بر فایل‌های ارزیابی فنی، شرکت باید مطابق راهنمای تکمیل فرم‌های ارزیابی امنیتی، اقدام به تکمیل و ارسال این فرم ها به سازمان نماید.**

پس از تکمیل کلیه فرم ها، در مجموع باید۳ لوح فشرده به صورت همزمان به سازمان تحویل داده شود. بدین صورت که شرکت متقاضی باید تمامی فایل‌های مربوط به Company.xsn و Service.xsn را که برای هرخدمت به‌طور جداگانه تکمیل شده است، به انضمام فایل های pdf شده هر یک از آن به همراه مدارک پشتیبان هر بخش ( شامل اسکن روزنامه رسمی، قراردادهای پرسنل، اساسنامه، گواهینامه های تحصیلی و آموزشی مرتبط افراد، لیست بیمه سه ماه اخیر، قرارداد های منعقد شرکت در حوزه های مربوطه و ...) به صورت pdf شده ، در دو حلقه لوح فشرده مشابه به سازمان تحویل نماید. علاوه براین، فایل مربوط به ارزیابی امنیتی (اعتباری) نیز دریک لوح فشرده جداگانه باید همراه با زونکن امنیتی به سازمان تحویل

داده شود. در جدول زیر اسامی مربوط به هرکدام از خدمات آمده است. درنام‌گذاری فایل Service.xsn به ازای هرخدمت، کلمه Service باید با نام متناسبی از جدول زیر جایگزین شود.

| حوزه | گرایش | | |
|---|---|---|---|
| | ردیف | نام خدمت | نام لاتین |
| خدمات مدیریتی افتا | ۱ | مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات | Standard |
| | ۲ | ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات | Audit |
| | ۳ | طرح ریزی معماری و زیرساخت امنیت | Planning |
| | ۴ | ارائه مشاوره حقوقی در حوزه امنیت فناوری اطلاعات | Legal |
| | ۵ | حوزه خدمات بیمه امنیت اطلاعات و ارتباطات | Insurance |
| خدمات عملیاتی افتا | ۱ | آزمون و ارزیابی امنیتی | Test |
| | ۲ | اندازی و مشاوره تیم پاسخ به رخداد و راه اندازی مرکز عملیات امن | Cert/Soc |
| | ۳ | امن سازی سامانه ها، زیرساخت ها و سرویس ها | Securing |
| | ۴ | امنیت فیزیکی و محیط پیرامونی | Physical–Sec |
| خدمات فنی افتا | ۱ | خدمات نصب و پشتیبانی تجهیزات امنیتی | Technical |
| | ۲ | خدمات ضدبدافزار | Anti Malware |
| خدمات آموزشی افتا | ۱ | خدمات آموزشی امنیت | Train |

**جدول شماره ۱: نام حوزه و گرایش خدمات**