ارائه نیازهای فناورانه حوزه امنیت
فناوری اطلاعات (افتا)

مرکز مدیریت راهبردی افتا
ریاست جمهوری

عنوان نیاز فناورانه

مشارکت فعال بخش خصوصی در اجرای «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» در حوزه

تامین خدمات

تامین محصولات

طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری

جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

فصل اول:

هدف و مأموریت‌های طرح، تعاریف، مخاطبان و نقشه راه اجرای طرح امن‌سازی

فصل دوم:

تبیین ۹ الزام محوری و اولویت‌دار برای امن‌سازی زیرساخت‌های حیاتی کشور

فصل سوم:

مدل بلوغ طرح امن‌سازی برای احصاء سطح بلوغ موجود و ترسیم سطح بلوغ مطلوب

فصل چهارم:

فرآیند ممیزی برای ارزیابی پیشرفت اجرای طرح در زیرساخت‌های حیاتی و نظارت بر اجرای آن

الزامات طرح


مدیریت مخاطرات
پایش و کنترل سایبری
مدیریت حوادث سایبری (IT/OT)
مدیریت تداوم کسب و کار
مدیریت تهدیدات بدافزاری
مدیریت زنجیره تامین

هدف از الزامات

مدیریت مخاطرات:

فرآیندی مستمر برای شناسایی، ارزیابی و مدیریت تهدیدات و آسیب‌پذیری‌های سازمان

پایش و کنترل سایبری:

پیشگیری از حوادث سایبری، تشخیص حملات سایبری و اعلام هشدار از طریق ایجاد مرکز عملیات امنیت در سازمان

مدیریت حوادث سایبری:

رسیدگی و مقابله با حوادث سایبری از طریق ایجاد واحد امداد سایبری در سازمان

مدیریت تهدیدات بدافزاری:

پیشگیری و مقابله با تهدیدات بدافزاری از طریق ایجاد واحد مقابله با بدافزار در سازمان

مدیریت تداوم کسب و کار:

مدیریت بازیابی، تداوم فعالیت سرویس‌های حیاتی کسب وکار سازمان در هنگام وقوع حوادث و شرایط بحرانی

هدف از الزامات

زیرساخت محرمانگی و استنادپذیری:

حفظ جامعیت، یکپارچگی و محرمانگی اطلاعات و تامین امنیت در تولید، انتقال، پردازش، نگهداری، امحاء و بکارگیری اطلاعات دارای طبقه‌بندی

مدیریت هویت و دسترسی:

مدیریت چرخه حیات هویت‌های دیجیتال، کنترل دسترسی، مدیریت رسانه‌های دیجیتال و غیر دیجیتال، ارتباطات راه دور و حفاظت فیزیکی

مدیریت زنجیره تامین:

امن‌سازی زنجیره تامین در تمامی مراحل نیازسنجی و طراحی، انتخاب تامین‌کنندگان، خرید/تولید داخلی و خارجی، انتقال مواد خریداری شده و انبارداری، نصب و راه‌اندازی و اجرا و راهبری، بهره‌برداری و خاتمه

آموزش و فرهنگ‌سازی:

ارتقاء دانش عمومی و تخصصی افتا در کشور و نهادینه‌سازی فرهنگ آن

مدل بلوغ امنیت سایبری

- ✓ شاخص‌ها و ویژگی‌هایی برای سنجش توانایی سازمان و با هدف ایجاد قابلیت سنجش پیشرفت سازمان
- ✓ ۱۰ دامنه منطبق با الزامات طرح که هریک شامل اهداف، سطوح و مجموعه‌ای از اقدامات
- ✓ هر دامنه به سطوحی به‌نام سطح شاخص بلوغ تقسیم می‌گردد.

۱- خط مشی امنیت اطلاعات سازمان	سطوح	فعالیت ها
	سطح ۱	SO-1-1-1- احصاء اهداف امنیت اطلاعات سازمان SO-1-1-2- احصاء عناوین و محورهای موردنیاز برای تدوین خط مشی امنیت اطلاعات
	سطح ۲	SO-1-2-1- تدوین خط مشی امنیت اطلاعات سازمان SO-1-2-2- تصویب خط مشی امنیت اطلاعات سازمان SO-1-2-3- ابلاغ و اطلاع‌رسانی خط مشی امنیت اطلاعات مصوب درون سازمان
	سطح ۳	SO-1-3-1- استقرار خط مشی امنیت اطلاعات در سازمان
	سطح ۴	SO-1-4-1- بازبینی دوره‌ای خط مشی امنیت اطلاعات و اطمینان از جامعیت و اثربخشی

شرح نیاز فناورانه

ارائه خدمات به زیرساخت‌های حیاتی با تاکید بر خدمات:

- امداد حوادث سایبری
- استقرار و راهبری مرکز عملیات امنیتی
- تحلیل شواهد دیجیتال و بدافزار
- امن سازی زیرساخت‌ها و سرویس ها در حوزه صنعتی–سایبری
- استقرار و ممیزی سیستم مدیریت امنیتی در حوزه صنعتی–سایبری
- فرهنگ سازی امنیت سایبری

شرح نیاز فناورانه

ارائه محصولات به زیرساخت‌های حیاتی:

- سامانه های مدیریت دارایی های سخت افزاری و نرم افزاری
- سامانه های مدیریت وصله
- UTM/NGFW
- WAF
- PAM
- NGAV
- تجهیزات امنیت صنعتی

فناوری‌ها و راه‌حل‌های نامطلوب

استفاده صرف از محصولات متن باز

عدم بروزرسانی قوانین

عدم بروزرسانی تکنیک‌های تشخیص و مقابله

نظام ارزیابی محصولات فتا و خدمات افتا

مرکز مدیریت راهبردی افتا

ارکان

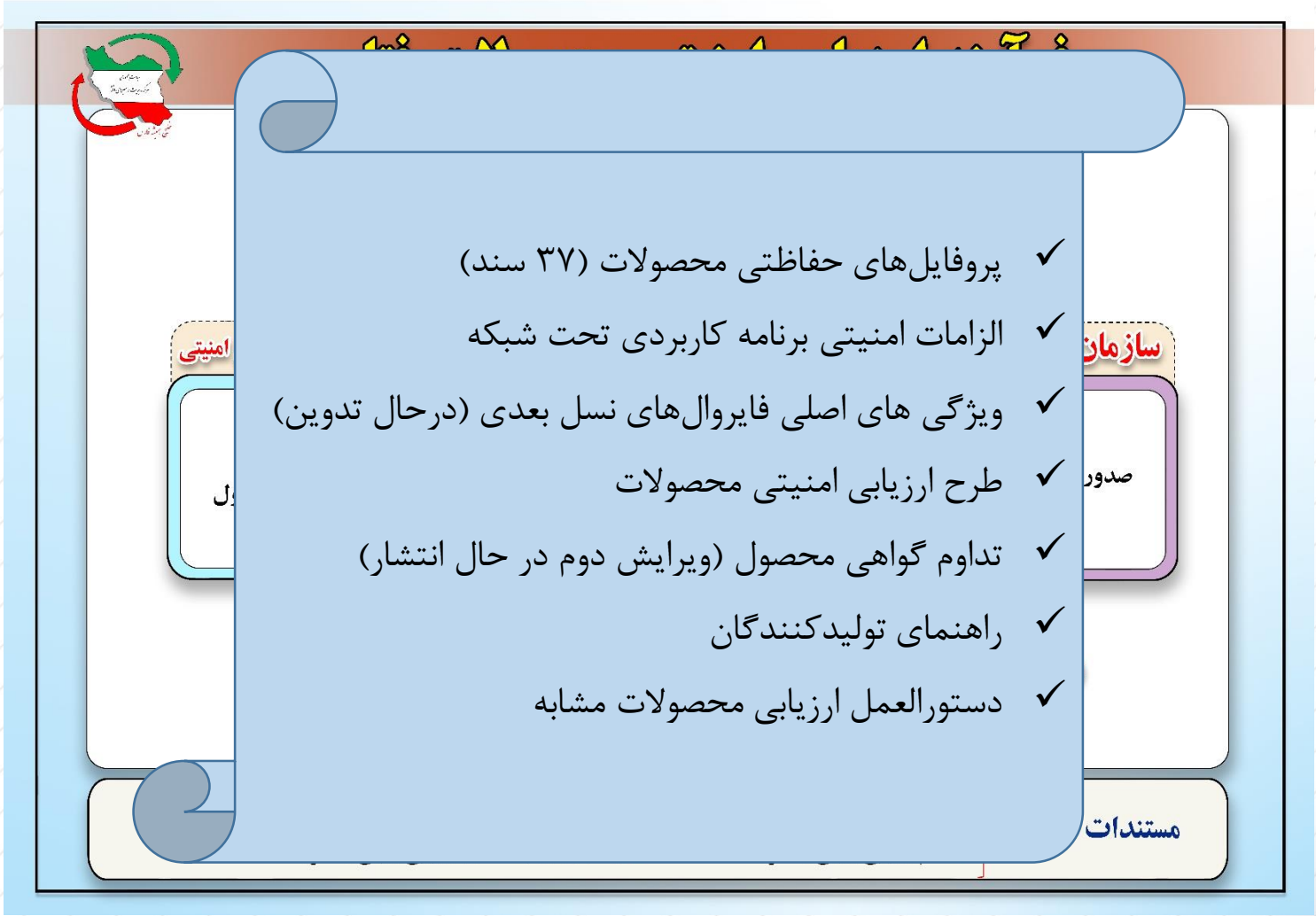
- ✓ نهاد اعتبار بخشی (مرکز مدیریت راهبردی افتا)
- ✓ نهاد صدور گواهی (سازمان فناوری اطلاعات)
- ✓ نهاد ارزیاب (آزمایشگاه یا ممیز)
- ✓ بخش خصوصی
  - ✓ تولید کنندگان محصولات
  - ✓ ارائه دهندگان خدمات

دسته بندی خدمات افتا

مدیریتی • مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات • ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات	**عملیاتی** • آزمون و ارزیابی امنیتی • آزمون و ارزیابی امنیتی مبتنی بر خرد جمعی و مسابقه • حفاظت ابری خدمات اینترنتی • 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
فنی • نصب و پشتیبانی محصولات فتا	**آموزشی** • برگزاری دوره‌های آموزشی افتا

- ✓ آیین نامه ساماندهی خدمات افتا (ویرایش دوم در مرحله تدوین نهایی)
- ✓ معرفی دوره‌های آموزشی افتا (ویرایش دوم ویرایش دوم در مرحله تدوین نهایی ر)
- ✓ راهنمای تعیین دامنه استقرار سیستم مدیریت امنیت اطلاعات
- ✓ الزامات اجرای خدمات (۶ سند)
  - الزامات استقرار سیستم مدیریت امنیت اطلاعات
  - الزامات دارندگان پروانه فعالیت خدمت آزمون و ارزیابی در اجرای پروژه‌های آزمون نفوذپذیری
  - الزامات امنیتی ارائه محصولات نرم افزاری سازمانی به زیرساخت‌های حیاتی
  - الزامات امنیتی زیرساخت‌های حیاتی در استفاده از محصولات نرم افزاری سازمانی
  - الزامات مربوط به شرکت‌های متقاضی پروانه خدمت ممیزی
  - الزامات اجرای خدمت برگزاری مسابقات کشف نقص امنیتی

مدل اجرایی - ادامه

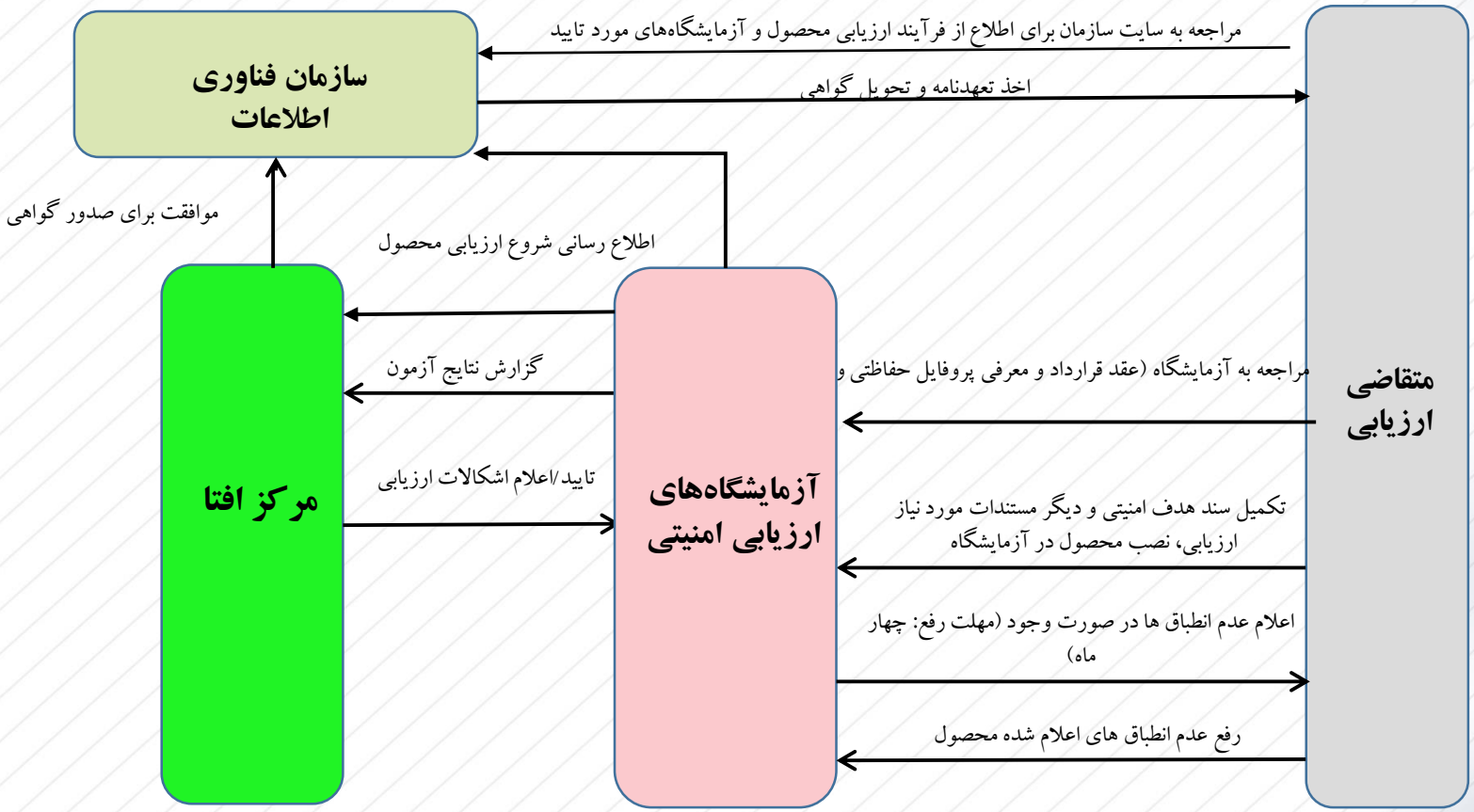


- ✓ پروفایل‌های حفاظتی محصولات (۳۷ سند)
- ✓ الزامات امنیتی برنامه کاربردی تحت شبکه
- ✓ ویژگی های اصلی فایروال‌های نسل بعدی (درحال تدوین)
- ✓ طرح ارزیابی امنیتی محصولات
- ✓ تداوم گواهی محصول (ویرایش دوم در حال انتشار)
- ✓ راهنمای تولیدکنندگان
- ✓ دستورالعمل ارزیابی محصولات مشابه

مدل اجرایی


ارزیابی و اعتباربخشی آزمایشگاه‌ها
آزمایشگاه
درخواست
آماده‌سازی آزمایشگاه
ارزیابی امنیتی محصول نمونه
پروانه آزمایشگاه
نظام ارزیابی آزمایشگاه‌ها
راهنمای آزمایشگاه ارزیابی امنیتی محصولات
طرح ارزیابی امنیتی محصولات
دستورالعمل ارزیابی محصولات مشابه (در حال انتشار)
مستندات
نظام اعتباربخشی آزمایشگاه‌ها

مراحل گام به گام فرایند ارزیابی امنیتی محصولات فتا



عنوان نیاز فناورانه

توسعه نظام ارزیابی امنیتی محصولات فتا و خدمات افتا

شرح نیاز فناورانه

توسعه در پوشش محصولات

توسعه در نوع ارزیابی محصولات

تدوین الزامات خدمات نوین

تدوین شاخص های ارزیابی فنی پروژه‌های افتایی

ایجاد نظام آموزش افتا

سطح بندی دارندگان پروانه فعالیت خدمات افتا