به نام خدا

عنوان سند:

Incident Management Procedure

دستورالعمل مدیریت حوادث امنیت اطلاعات

۱- هدف (Purpose)

هدف از این دستورالعمل، تعریف فرآیند استاندارد برای شناسایی، گزارش‌دهی، ارزیابی، پاسخ، مهار و بازیابی حوادث امنیت اطلاعات به‌منظور کاهش اثرات منفی، حفظ تداوم کسب‌وکار و بهبود مستمر سیستم مدیریت امنیت اطلاعات (ISMS)است. این دستورالعمل در راستای الزامات ISO/IEC ۲۷۰۰۱ ، چارچوب NIST Cybersecurity Frameworkو اصول حاکمیت COBIT تدوین شده است.

۲- دامنه کاربرد(Scope)

این دستورالعمل برای کلیه کارکنان، مدیران، پیمانکاران و اشخاص ثالثی که به سیستم‌ها و اطلاعات شرکت دسترسی دارند، قابل اجرا است و تمامی حوادث مرتبط با محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را پوشش می‌دهد.

۳- تعاریف (Definitions)

- **حادثه امنیت اطلاعات** :هر رویداد یا مجموعه‌ای از رویدادها که می‌تواند محرمانگی، یکپارچگی یا دسترس‌پذیری اطلاعات را تهدید کند.
- **رویداد امنیتی** :وقوع قابل مشاهده در یک سیستم که لزوماً منجر به حادثه نمی‌شود.
- **CSIRT**:تیم پاسخ‌گویی به حوادث امنیت اطلاعات.

۴- نقش ها و مسئولیت ها (Roles & Responsibilities)

٤_١ کارکنان و کاربران

- رعایت الزامات امنیت اطلاعات
- گزارش فوری هرگونه رویداد یا حادثه مشکوک

٤_٢ مسئول امنیت اطلاعات (ISMS)

- دریافت و ثبت حوادث امنیتی
- ارزیابی اولیه و طبقه‌بندی حادثه
- هماهنگی پاسخ به حادثه

٤_٣ تیم پاسخگویی به حادثه

- تحلیل فنی حادثه
- مهار و رفع حادثه
- ارائه گزارش نهایی و درس‌آموخته‌ها

٤_٤ مدیریت ارشد

- حمایت از فرآیند مدیریت حادثه
- تصمیم‌گیری در حوادث بحرانی

۵- طبقه بندی حوادث امنیت اطلاعات (Incident Classification)

حوادث امنیت اطلاعات بر اساس شدت و تأثیر به سطوح زیر تقسیم می‌شوند:

سطح	توضیح
پایین	تأثیر محدود، بدون اختلال جدی
متوسط	اختلال محدود در سرویس‌ها
بالا	تأثیر قابل توجه بر کسب‌وکار
بحرانی	توقف سرویس‌های حیاتی یا نشت گسترده اطلاعات

۶- فرآیند مدیریت حوادث امنیت اطلاعات

٦_١ شناسایی و گزارش‌دهی (Identification & Reporting)

- شناسایی حوادث از طریق کاربران، ابزارهای پایش یا گزارش اشخاص ثالث
- ثبت حادثه درIncident Log

٦_٢ ارزیابی و تحلیل (Assessment & Analysis)

- تعیین نوع، دامنه و شدت حادثه
- تصمیم‌گیری در خصوص فعال‌سازیCSIRT

۶-۳ پاسخ و مهار (Response & Containment)

- اجرای اقدامات فوری برای جلوگیری از گسترش حادثه
- حفظ شواهد در صورت نیاز قانونی

۶-۴ بازیابی (Recovery)

- بازگردانی سیستم‌ها و سرویس‌ها به وضعیت عادی
- اطمینان از رفع آسیب‌پذیری‌های شناسایی‌شده

۷- ارتباطات و گزارش‌دهی (Communication & Reporting)

در حوادث با سطح بالا و بحرانی، اطلاع‌رسانی به مدیریت ارشد و در صورت لزوم مراجع ذی‌ربط (مطابق الزامات قانونی کشور) انجام می‌شود. کلیه گزارش‌ها به‌صورت مستند نگهداری می‌شوند.

۸- انطباق با چارچوب‌ها و استانداردها

- ISO/IEC ۲۷۰۰۱: بندهای مرتبط با Incident Management و بهبود مستمر
- NIST CSF: توابعDetect ، RespondوRecover
- COBIT ۲۰۱۹: اهداف (Managed Incidents) DSS۰۲ و(Risk Management) APO۱۲

۹- آموزش و آگاهی

کارکنان به‌صورت دوره‌ای در خصوص نحوه شناسایی و گزارش حوادث امنیت اطلاعات آموزش می‌بینند.

۱۰- بازبینی و بهبود

این دستورالعمل حداقل سالی یک‌بار یا پس از وقوع حوادث مهم بازبینی و در صورت نیاز به‌روزرسانی می‌شود.

تصویب‌کننده :مدیریت ارشد شرکت
تاریخ اجرا
نسخه