به نام خدا

عنوان سند:

Asset Inventory & Classification Procedure

سند شناسایی و طبقه‌بندی دارایی‌ها

۱- هدف (Purpose)

هدف از این سند، ایجاد یک روش ساخت‌یافته برای شناسایی، ثبت، مالکیت و طبقه‌بندی دارایی‌های اطلاعاتی سازمان به‌منظور پشتیبانی از مدیریت ریسک امنیت اطلاعات و پیاده‌سازی مؤثر ISMS است. این سند در راستای الزامات ISO/IEC ۲۷۰۰۱و همسو با چارچوب NIST CSF و اصول حاکمیت COBIT تدوین شده است.

۲- دامنه کاربرد(Scope)

این دستورالعمل کلیه دارایی‌های اطلاعاتی سازمان، اعم از دارایی‌های دیجیتال، فیزیکی، نرم‌افزاری، سخت‌افزاری و اطلاعاتی را پوشش می‌دهد و برای تمامی واحدها، کارکنان و اشخاص ثالث مرتبط با این دارایی‌ها لازم‌الاجرا است.

۳- انواع دارایی‌ها(Asset Categories)

دارایی‌های سازمان در دسته‌های زیر شناسایی و ثبت می‌شوند:

- اطلاعات (داده‌های مشتریان، اسناد مالی، پایگاه‌های داده)
- نرم‌افزارها (سیستم‌های کاربردی، سیستم‌عامل‌ها، وب‌سایت‌ها)
- سخت‌افزارها (سرورها، رایانه‌ها، تجهیزات شبکه)
- خدمات (سرویس‌های ابری، خدمات برون‌سپاری‌شده)
- منابع انسانی (دانش و مهارت کارکنان کلیدی)
- دارایی‌های فیزیکی و محیطی (اتاق سرور، تجهیزات پشتیبان)

۴- فرآیند شناسایی دارایی‌ها(Asset Identification Process)

- شناسایی دارایی‌ها توسط واحدهای مربوطه
- ثبت دارایی در فهرست دارایی‌ها(Asset Register)
- تعیین مالک دارایی
- تعیین محل نگهداری یا استفاده از دارایی

۵- طبقه‌بندی دارایی‌ها(Asset Classification)

دارایی‌ها بر اساس سطح حساسیت به چهار سطح زیر طبقه‌بندی می‌شوند:

سطح	توضیح
عمومی(Public)	قابل افشا بدون آسیب
داخلی(Internal)	مخصوص استفاده داخلی
محرمانه(Confidential)	نیازمند حفاظت ویژه
بسیار محرمانه(Restricted)	افشای آن موجب آسیب جدی می‌شود

معیار طبقه‌بندی بر اساس تأثیر بر محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات تعیین می‌گردد.

۶- مالکیت و مسئولیت دارایی‌ها(Asset Ownership)

برای هر دارایی یک مالک مشخص می‌شود که مسئول موارد زیر است:

- اطمینان از طبقه‌بندی صحیح دارایی
- تعیین کنترل‌های امنیتی مناسب
- بازبینی دوره‌ای وضعیت دارایی

۷- نگهداری و به‌روزرسانی فهرست دارایی‌ها

- حداقل سالی یک‌بار بازبینی شود
- در صورت تغییرات مهم (افزودن، حذف یا تغییر دارایی) به‌روزرسانی گردد

۸- ارتباط با مدیریت ریسک و کنترل‌ها

اطلاعات ثبت‌شده در Asset Inventory به‌عنوان ورودی اصلی فرآیند ارزیابی ریسک امنیت اطلاعات استفاده می‌شود. انتخاب کنترل‌های امنیتی در SoA بر اساس نوع و طبقه‌بندی دارایی‌ها انجام می‌گردد.

۹- انطباق با استانداردها و چارچوب‌ها

- ISO/IEC ۲۷۰۰۱: کنترل‌های مرتبط با Asset Management و Information Classification
- NIST CSF: تابع Identify (Asset Management)

- COBIT ۲۰۱۹: اهداف APO۰۳ (Enterprise Architecture) وAPO۱۲ (Risk Management)

۱۰- لیست دارایی‌ها (Asset Inventory)

ID	نام دارایی (Asset Name)	دسته‌بندی	مالک (Owner)	مکان	C (محرمانگی)	I (یکپارچگی)	A (دسترس‌پذیری)	ارزش دارایی (Max)
AST-01	دیتابیس تراکنش‌های مشتریان	اطلاعات/داده	مدیر فنی	سرور دیتاسنتر	۳ (High)	۳ (High)	۳ (High)	۳
AST-02	سورس‌کد اپلیکیشن کیف پول	نرم‌افزار	مدیر توسعه	گیت‌لب (GitLab)	۳ (High)	۲ (Medium)	۲ (Medium)	۳
AST-03	ایمیل‌های سازمانی پرسنل	سرویس	مدیر IT	ابری/هاست	۲ (Medium)	۲ (Medium)	۲ (Medium)	۲
AST-04	سرور فیزیکی HP (DL380)	سخت‌افزار	مدیر زیرساخت	اتاق سرور	۱ (Low)	۱ (Low)	۳ (High)	۳
AST-05	پرسنل واحد مالی	نیروی انسانی	مدیر HR	طبقه دوم	۲ (Medium)	۲ (Medium)	۲ (Medium)	۲

۱۱- لیست دارایی‌ها (Asset Register)

شماره	دارایی	مالک	اهمیت (محرمانگی/یکپارچگی/در دسترس بودن)	مکان
۱	پایگاه داده مشتریان	تیم IT	بالا/بالا/بالا	سرور داخلی + ابر
۲	کد منبع نرم‌افزار	تیم توسعه	بالا/بالا/متوسط	Gitداخلی
۳	سرورهای وب/اپ	تیم عملیات	متوسط/بالا/بالا	دیتاسنتر تهران
۴	لپ‌تاپ کارکنان IT	کارکنان	متوسط/متوسط/متوسط	دفتر/دورکاری
۵	ایمیل سازمانی	تیم IT	بالا/متوسط/بالا	سرویس ایرانی

۱۲- بازبینی و بهبود

این سند حداقل سالی یک‌بار یا در صورت تغییرات اساسی در دارایی‌ها، فناوری یا ساختار سازمان بازبینی می‌شود.

تصویب‌کننده :مدیریت ارشد شرکت
تاریخ اجرا
نسخه