EGNYTE

Information Classification Levels

LEVEL 00

Public

Information that is already public.

Example:
Job postings, (released) advertising, organization contact information, other public domain information

User Scope: Public

Solution:
Internet web sites

LEVEL 01

Routine (Internal Use Only)

Routine information available to all employees that might cause risk if exposed externally.

Example:
Employee contact information, benefits, routine business reports, routine memos, org charts, business calendars

User Scope:
All employees and contractors

Standard Regulations:
Responsible business practices, NIST 800-53, ISO 27001

Solution:
Egnyte Enterprise Lite (Collaboration)
Dropbox, Box, OneDrive, etc.

LEVEL 02

Sensitive (Confidential)

Business and employee information that would cause material harm if exposed.

Example:
Roadmaps and product plans, pricing plans. Financial information, employee personal information, health information customer information

User Scope:
Employees within a group or department

Standard Regulations:
GDPR, HIPAA, PCI-DSS, SEC Rule 240 (retention), Gramm-Leach-Bliley

Solution:
Egnyte Enterprise (governance)

LEVEL 03

Executive (Restricted)

Information on large deals that would cause existential harm to the organization if exposed.

Example:
Mergers, acquisitions, funding rounds, due diligence, partnerships, large deals

User Scope:
Senior level executives, finance, and legal staff

Standard Regulations:
SEC rules 17a, 31a-2, 204-2, Sarbanes-Oxley

Solution:
Separate Egnyte domain

LEVEL 04

Government Controlled Unclassified Information (CUI)

Information that could cause risk to national security if exposed.

Example:
Government contracts, specifications for government products and services, schedules

User Scope:
Specific employees with need to know

Standard Regulations:
CMMC, NIST 800-171, FedRAMP

Solution:
Egnyte for CMMC 2.0 Compliance

LEVEL 05

Government Classified (Secret, Top Secret, Top Secret SCI)

Information that would cause harm to national security if exposed.

Example:
Intelligence assets, military plans and systems, etc.

User Scope:
Cleared employees with security credentials

Standard Regulations:
Various DoD, DoE, and Intelligence directives

Solution:
Approved air-gapped systems, SIPR, NIPR