# Security Awareness: Information Protection

Information protection is critical to prevent unauthorized access and data leakage. Companies categorize information protection into three sections: public, confidential and internal. All three categories of data are crucial to the company and must be protected. Protecting company data depends on employees' access to data, role, department and compliance requirements.

**Note: If you feel information has been leaked, please let your manager or your company's help desk know immediately. Never hesitate to report any suspicion or any data leakage.**

### Precautions to prevent information leakage:

- Don't email sensitive information to personal or external email addresses
- Don't store company information on personal devices or cloud storage sites
- Don't vary from standard procedures when transferring information
- Don’t take sensitive or classified calls in public
- Don't use company-issued devices for personal business
- For more information, see your company policy on data loss prevention

## Types of Company Data

Company data categorization depends on the severity of damage if the information is leaked.

### Public

This information is publicly available and not subject to a nondisclosure agreement (NDA). This information doesn't pose risks to the organization.

- Company website
- Company social media
- Information in the news

## Types of Company Data *(continued)*

### Confidential

This data is restricted to authorized personnel only. Unauthorized disclosure could cause harm and violate laws (consult privacy laws for different countries and regions — e.g., California, Europe, Taiwan, etc.). Information that should be labeled as confidential includes:

- Company infrastructure and network diagrams
- Policies and procedures
- Financial reports
- Customer confidential data (does not include customer personally identifiable information, or PII)

### Internal

This data is the most sensitive and is limited to authorized people who have a need to know. If the information is leaked or shared improperly, it could lead to serious harm. Examples that should be labeled as company internal confidential information include:

- Employee personal files
- Customer PII
- Encryption key
- Source code
- Vulnerability information
- Project plans/product development roadmaps

**If you are unsure if you might be sharing company information, please ask your manager or security team**.

## Traveling

While traveling outside of your assigned work location, be sure to let your help desk know and follow company policy. Also, see your company's guidance on how to best protect information while traveling.

**Get more resources from CrowdStrike for creating your own Security Awareness Program →**

# About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

**CrowdStrike: We stop breaches.**

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram