Ironcore Resources

ZERO TRUST AWARENESS: DATA CLASSIFICATION

DATA CLASSIFICATION AND ZERO TRUST

Data classification is a crucial aspect of any security strategy, but it is especially important in a Zero Trust framework. In a Zero Trust model, all assets and resources are considered untrusted until they are verified and approved, making it essential to have a clear understanding of the type of data that is being stored, processed, and transmitted.

WHY IT'S IMPORTANT

COMPLIANCE:

Many industries and countries have specific regulations around the protection of personal and sensitive information. By classifying data, organizations can comply with these regulations and avoid potential fines or legal penalties. Examples include: HIPAA protection of patient health information and PCI DSS rules on handling credit card data.

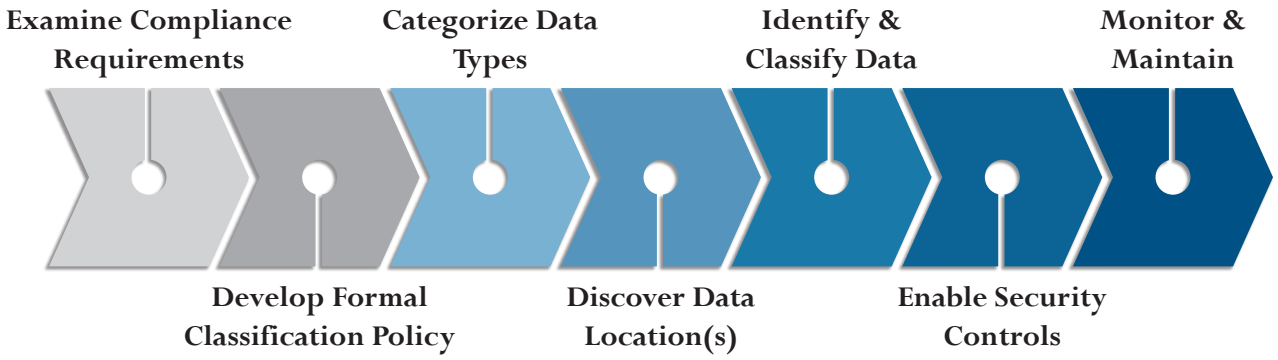
SECURITY:

Data classification enables organizations to identify sensitive or confidential data. With a clear understanding of data classifications, organizations can ensure that the appropriate security measures are in place to protect it. This includes implementing access controls, encryption, and monitoring for any unauthorized access or use.

VISIBILITY:

Organizations gain greater visibility into their information assets enabling more effective management and protection of data. Increased visibility empowers timely detection and response to any potential security threats, reducing the risk of a data breach and the effort & costs associated with mitigating the issue.

DATA CLASSIFICATION STEPS



IRONCORE
STRONG · TRUSTED · SECURE

www.ironcore-inc.com
zerotrust@ironcore-inc.com / 608-779-9400

DATA CATEGORIZATION EXAMPLE

Classification categories vary depending on industry and product/service offerings, however it is generally recommended to utilize three to four classification categories. Categories should identify data sensitivity and business impact in order to enforce proper security controls.

PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
			
INSIGNIFICANT IMPACT	**LOW IMPACT**	**MEDIUM IMPACT**	**HIGH IMPACT**
Data may be freely disclosed to the public.	*Internal data not meant for public disclosure.*	*Sensitive data that if compromised could negatively affect operations.*	*Highly sensitive data that if compromised could cause financial or legal impact.*
Marketing materials, published data, price lists, etc.	Business processes and procedures, battlecards, sales playbooks, etc.	Contracts, staff HR data, financial data, etc.	Data subject to regulations, IP, trade secrets, etc.

CONSIDERATIONS

RISK-BASED SECURITY

The level of protection applied to a particular piece of data is based on its classification. By understanding the organizational value and location of data, appropriate policies and procedures can be implemented based on possible impact of exposure. Policies and procedures should provide guidelines for handling data, solidify employee roles and responsibilities, identify desired security controls, and be easily interpreted. This reduces the risk of a data breach and ensures sensitive information is protected to the fullest extent possible.

MANAGING DATA OVER TIME

It is important to note that data classification is not a one-time process, but rather an ongoing effort that requires regular review and updates. This is because new information is constantly being created and the sensitivity of existing data can change over time. By having a clear understanding of the classification of their data, organizations can ensure that appropriate measures are taken to protect it as it evolves. This helps organizations to stay up-to-date with the latest security measures and regulations.

SUBSCRIBE TO OUR BLOG

Scan the QR Code or visit www.ironcore-inc.com/blog to follow more educational series like this.