Data Security Policy & WipeDrive

Corporations manage large volumes of data for internal and external consumption. This information can be customer details, partner contracts, personal health information, employee data, financial information and many other forms of data.

This information is central to a business's internal performance and relationships with customers and other partners. This data has such a high value it is a target for exploitation and attack. To protect this data government regulations, like GDPR, have been instituted to create data security requirements for organizations.

The data security policy is the internal rules to manage the data and applicable laws and regulations.

DATA SECURITY POLICY

The components of a data security policy cover the information stored in an organization and provides regulated access to employees and others that need access to the information. The data security policy should also include data and network segmentation, identity and access management, and the organizations' entire security posture, monitoring all activity across every IT asset looking for abnormal and/or suspicious activity and activity patterns.

WHAT IS A DATA SECURITY POLICY?

A data security policy is a document that states in writing how an organization safeguards data from threats to personal, professional and institutional interests and complies with applicable laws.

Once the policy is instituted and implemented across the enterprise, it should be reviewed at least twice a year to bring it current. Organizations that are serious about preventing cybercrime must also consider the important link between data security and data privacy and create the custom policy that will safeguard the data they're entrusted with is used properly, legitimately and with the confidence that company and customer data is kept safe and secure.

IMPORTANT ELEMENTS OF A DATA SECURITY POLICY

1. **Accountability for Data Security –** An organization should properly communicate to IT staff, workforce and management their responsibilities and what requirements are expected of them. The data should be classified in various classes so that they can be easily distinguished by all employees. The employees should be trained on how to manage the different data classes, how to handle each class and the distribution limitations for each class. The following data classes should be included in the policy:
   - **a.** Confidential data
   - **b.** Data that is meant to be sent internally within the company
   - **c.** General data
   - **d.** Data that is meant to be sent outside the company
2. **Network Services Policy –** The data security policy should communicate how remote access and IP addresses are managed and configured. Network hardware, like routers and switches, should also be addressed. The detection and reporting of network intrusions should also be dictated in this policy.

3. Vulnerability Scanning – Routine vulnerability scanning should be scheduled and ordered by the policy. As should the reporting for any discovered vulnerabilities.

4. Managing Patches – The elimination of vulnerabilities by implementing code, and how/when these patches are pushed into the live environment should be a part of the data security policy.

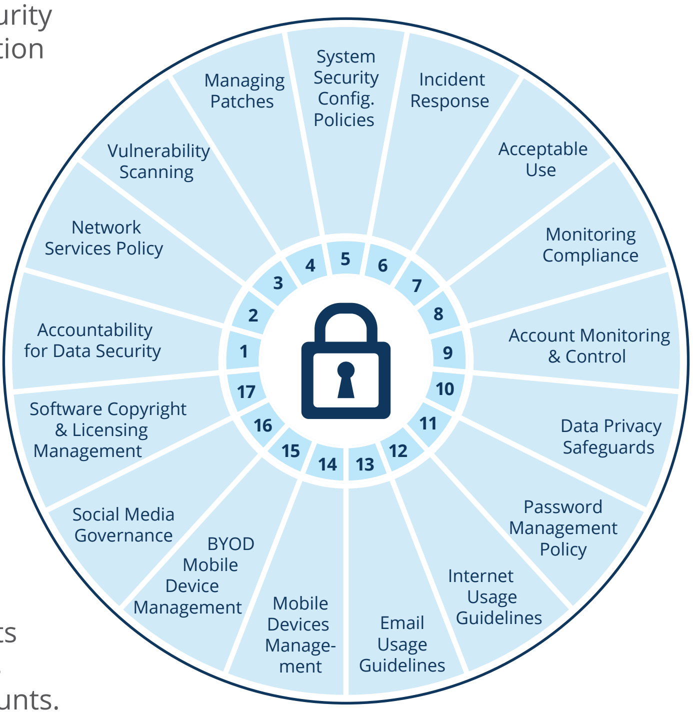
5. System Security Configuration Policies – The servers and operating systems should have their security configuration requirements mandated by the data security policy. As should the management of passwords, accounts, firewalls, database access and antivirus policies. It is important to note that all systems running on your internal network must abide by these policies.

6. Incident Response – Proper steps for handling a security breach should be described and detailed. The evaluation and reporting components of the incident and the resolution should also be mandated.

7. Acceptable Use – Employees should be trained and communicated with precise explanations of what constitutes acceptable use. Typically, organizations require employees to sign an acceptable use policy so disciplinary action can be pursued, if necessary.

8. Monitoring Compliance – Compliance audits should be performed by staff and management to ensure employees are abiding by the data security policy. These audits should be performed on a regular schedule.

9. Account Monitoring & Control – The tracking of employee's access to any data is an important part of a data security policy. This tracking will provide insights into how has what data access. Specific IT technicians should be tasked to monitor and control all user accounts.


1 Accountability for Data Security
2 Network Services Policy
3 Vulnerability Scanning
4 Managing Patches
5 System Security Config. Policies
6 Incident Response
7 Acceptable Use
8 Monitoring Compliance
9 Account Monitoring & Control
10 Data Privacy Safeguards
11 Password Management Policy
12 Internet Usage Guidelines
13 Email Usage Guidelines
14 Mobile Devices Manage-ment
15 BYOD Mobile Device Management
16 Social Media Governance
17 Software Copyright & Licensing Management

10. Data Privacy Safeguards – An organization's data must only be used in ways that conform to all applicable laws and regulations. It is imperative that the privacy policy by followed by employees to keep customer identity and data confidential.

11. Password Management Policy – Any employee or temporary employee with access to corporate resources should be trained on and follow a password policy. Passwords should never be shared, and password intricacy should also be dictated.

12. Internet Usage Guidelines – The misuse of the internet by an employee can place a company in an awkward, or even illegal, position. Employees should be trained on appropriate and inappropriate internet usage in the workplace. Security constraints should also dictate how internet guidelines are formulated.

13. Email Usage Guidelines – The misuse of email is a major cause of data breaches by accidentally downloading viruses, trojans and malware. Email usage should be standardized and training provided on the use of emails, message content, encryption and file retention.

14. **Mobile Devices Management –** Organizations that provide mobile devices to employee should create a formal process for the management, clearing and decommissioning of the devices. Employees should also be required to protect their devices from theft with password and other protection devices.

15. **BYOD Mobile Device Management –** Employee devices that connect to a company's internal network, applications or infrastructure should be clearly policed to ensure company controls are met by the devices. Employees should be clearly trained on the appropriate use and access of personal devices on an organization's network. All these requirements should be documented in the data security policy.

16. **Social Media Governance –** An organization should implement a social media policy to protect its online activities, promotions and communications to customers. A strong governance policy should also train employees on effective communication on social media.

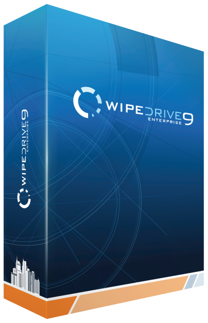
17. **Software Copyright and Licensing Management –** The data security policy should limit the download and use of software that may be in violation of copyright laws. The employees in an organization should be properly trained on which software tools can and cannot be implemented on company IT assets. All software should be reviewed and approved by management.

WIPEDRIVE'S ROLE IN A DATA SECURITY POLICY

WipeDrive is a central component for data security policy's at the end of IT assets lifecycle. Any data-bearing device that is decommissioned or leaves a facility should be wiped clear of any information using the NIST overwrite pattern. This level of data eradication will protect the organization from accidental data breaches and the WipeDrive audit report can be used for internal asset management reports and ERP systems.

WIPEDRIVE IMPLEMENTATION BY GLOBAL CORPORATIONS

Large global organizations have discovered that WipeDrive can be pre-configured for uniform distribution throughout their organizations. This pre-configuration of settings ensures that all departments implement the correct erasure pattern, all reports are identical and an additional 32 settings can be set by management to meet their internal Data Security Policy requirements.



WipeDrive Enterprise provides a secure erasure solution for data at rest and for IT assets at end of life. With deployments in global corporations, WipeDrive provides the features necessary to meet your internal data security policy. For more information, contact the WipeDrive Sales Team at +44 (0) 345 340 3105