ManageEngine
DataSecurity Plus

Data security Checklist

Protecting data in all its states—at rest, in use, and in motion—requires administrators to implement security measures specific to their organization's needs. These include multiple processes ranging from detecting critical data to enabling post-breach root cause analysis. Not implementing these processes can have devastating consequences for organizations, including damaging data breaches and massive non-compliance penalties.

Use this data security checklist template to avoid security incidents and gain more control over how your data is stored, accessed, and transferred.

Data security checklist template

Step 1: Inventory critical data assets	
What to do	**How to do it**
☐ Define data discovery rules	Know what type of sensitive data you collect and store. Create a combination of regular expression and keyword match data discovery rules specific to your organization.
☐ Scan data stores for sensitive data	Scan data stores (including images and audio files) for sensitive data instances that match the configured rules. Ensure that you avoid overloading systems by pausing scans during business hours and deploying distributed scanning methods.
☐ Employ data validation methods	Use a combination of checks, proximity scanning, and compound-term processing to validate the data discovery results.
☐ Create compliance-specific discovery policies	Create policies for the regulations you are obliged to adhere to. This will aid in preventing non-compliance and also speed up reporting.
☐ Map out the discovered sensitive data	Know where your most critical data is stored. Maintain an inventory of sensitive data instances and keep it up to date by scanning files once they are created and modified.
☐ Categorize and classify sensitive data	Use both automated and manual classification methods to tag files based on their sensitivity. This will help you define data protection policies based on these tags.
☐ Build file-based and user-based risk profiles	Find out which storage location is most densely comprised of sensitive data and which employees store the most personal information. Analyze data discovery results and create detailed risk profiles for your storage repository and users.

Step 2: Evaluate data security risks	
What to do	**How to do it**
☐ Locate sensitive data stored outside designated repositories	Ensure that critical data is stored only where it should be. Establish workflows to move it from open shares and other unsecure folders to more protected locations.
☐ Remove sensitive files stored beyond their retention periods	Avoid non-compliance penalties by listing old, stale, unmodified files and removing or archiving them if they are obsolete.
☐ Detect and discard duplicate copies of critical files to maintain the integrity of master files	Improve data storage practices by listing and removing duplicate copies of files.
☐ Verify role-based access control and least privilege	Scrutinize NTFS and share permissions to verify that critical data is only accessible by those who require access to it for their work
☐ Perform periodic access rights reviews	Prevent privilege creep and excessive access rights by periodically reviewing permissions.
☐ Spot and fix instances of broken inheritance	Fix security vulnerabilities like broken inheritances and openly accessible folders.
☐ Limit the visibility of sensitive data	Redact or anonymize instances of personal information from documents to prevent unnecessary disclosure.

Step 3: Monitor access to critical data	
What to do	**How to do it**
☐ Track changes made to critical files	Track file read, create, modify, overwrite, move, rename, delete, and permission change events in real time.
☐ Monitor file integrity	Monitor risky activity such as failed attempts to read, write, or delete files, and critical changes made outside business hours.
☐ Set alerts for high-risk file modification, move, delete, and permission change actions	Set up triggers to receive instant notifications about potential data security threats and anomalous file activities.

☐ Implement comprehensive antivirus and anti-malware systems	Watch out for infected files, indicators of ongoing malware attacks, and other critical signs of impending data breaches with up-to-date malware detection tools.
☐ Deploy automated security incident response systems	Configure responses to halt the spread of ransomware infections, shut down infected devices, disconnect rogue users sessions, and more based on the security alert triggered.
☐ Automate access reporting for compliance regulations	Generate audit-ready reports to comply with the GDPR, PCI DSS, HIPAA, and other regulations. Store historical audit data for legal and forensic requirements.

Step 4: Regulate endpoint activity	
What to do	**How to do it**
☐ Monitor the use of removable storage media	Track and analyze the use of removable devices—including removable media devices such as USBs or mobile phones—in your network.
☐ Control the use of USB drives with allow lists and block lists	Restrict the use of USB devices by selectively blocking read, write, or execute actions in USBs, and prevent unauthorized use by using allow and block lists.
☐ Manage the use of endpoints	Block employees from using Wi-Fi, Bluetooth devices, CD or DVD drives, and other endpoints to limit the potential attack surface for data security threats.
☐ Prevent data leaks with policies for data exfiltration attempts via endpoints	Customize data leak prevention (DLP) policies for organization-specific use cases.
☐ Prevent classified files from being removed from the network	Map DLP policies to file classification tags to granularly prevent restricted-use files from being removed from the organizational network via email, USB drives, etc.
☐ Scan for vulnerabilities periodically	Assess applications and endpoint devices for vulnerabilities and remediate issues before they can be used to carry out data theft.

☐ Improve user awareness	Train your end users about social engineering attacks to prevent accidental data leaks from endpoints.
☐ Review and improve DLP processes	Leak prevention is a process that should be kept in line with changing business conditions and needs. Continuously monitor the DLP strategy you've implemented and improve it wherever necessary.

Step 5: Deploy cloud protection	
What to do	**How to do it**
☐ Audit cloud application usage	Use deep packet inspection to audit how actors access cloud applications. Analyze upload, download, and other activity details across cloud storage and platforms such as Box, Dropbox, and Microsoft 365.
☐ Evaluate the risk associated with accessing web applications	Score websites based on their reputation, and take measures to limit the use of low-reputed websites.
☐ Track accesses to shadow IT applications	Monitor users who access shadow IT applications and gather details on how often they access them.
☐ Filter unsecure webpages	Enforce access control measures across cloud applications to ensure that employees do not interact with sites that incite violence, host inappropriate content, spread malware, initiate spam campaigns, promote gambling, etc.
☐ Control file uploads and downloads	Prevent users from uploading sensitive files to cloud repositories and from downloading potentially malicious files.

Disclaimer: Data security requires a variety of solutions, processes, people, and technologies. This checklist is provided for informational purposes only and should not be considered as legal advice. ManageEngine makes no warranties, express, implied, or statutory, as to the efficacy of the information in this material.

How ManageEngine can help you streamline data security processes

Reinforce your measures to secure organizational data in all its states—at rest, in use, and in motion—with ManageEngine DataSecurity Plus. DataSecurity Plus is a unified data visibility and security platform that:

- Audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations.
- Analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities.
- Helps users assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI.
- Prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

Next steps

See how you can leverage DataSecurity Plus in your environment.

Schedule a demo
manageengine.com/data-security/demo-form.html

Download the free trial
manageengine.com/data-security/download.html

Contact us
support@datasecurityplus.com