Data Loss Prevention (DLP) policy for CyberSecure Systems Ltd..

Introduction

Data Loss Prevention (DLP) is defined as a strategy that detects potential data breaches or data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in-motion (network traffic), and at rest (data storage).

Data Loss Prevention is also synonymous with the term Data Leakage Prevention. These terms are often used interchangeably, however, Data Loss Prevention is the common term used by DLP solution providers today.

Purpose of DLP

GAIL(India) Ltd. (GAIL) must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting its customers. The protection of in-scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical. This policy supports a range of general regulations by restricting access to data hosted in GAIL Primary datacenter at Noida (DC), Nearline DC at GTI, Noida (NDC) and disaster recovery Centre at Jaipur (DR).

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, as defined by numerous compliance standards, industry best practices and associated processes.

- Following are the Core components of DLP:
- DLP for the Endpoint: Data residing on the desktop, laptop, USB storage, virtual desktops
- DLP at Rest or for Storage: Usually unstructured data residing on a server or structured data residing on Databases.
- DLP for Network: Data that transits or leaves the network to the Internet.
- DLP Policy: Employee requirements

All the employees of GAIL need to complete its security awareness training and agree to IT acceptable use policy.

If any unknown, un-escorted or unauthorized individual is found in DC/NDC/DR, it should be immediately notified to Security department.

Visitors to DC/NDC/DR must be escorted by FMS support Engineer at all times. Visitor must be restricted into appropriate areas.

Employees are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by GAIL. For example, the use of external e-mail systems not hosted by GAIL to distribute data is not allowed.

Please keep a clean desk. To maintain information security, Employee need to ensure that all printed in scope data is not left unattended at your workstation.

Employee needs to use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.

Superannuated/Terminated employees will be required to return all official records. This requirement should be part of the employee onboarding process.

Employee must immediately notify the authority in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc.).

In the event that Employee finds a system or process which employee suspect is not compliant with this policy or the objective of information security employee have a duty to inform the appropriate authority so that they can take appropriate action.

If employee have been provided facility to work remotely, employee must take extra precaution to ensure that data is appropriately handled.

Employee should ensure that GAIL assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.

Data that must be moved from DC/NDC/DR is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email, etc.). GAIL will provide employee with systems or devices that fit this purpose. Employee must not use other mechanisms to handle in scope data. If employee have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with IT department.

DLP policy: Data in Motion

DLP solution will be configured at the endpoints to identify data in motion to Browsers, IM Clients, E-mail clients, Mass storage devices and writable CD media, etc.

- DLP technology will scan for data in motion and will identify specific content, i.e.:
- E-mail addresses, names, addresses and other combinations of personally identifiable information
- Documents that have been explicitly marked with the ‘GAIL Confidential’ string.

DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through change process

and with approval, toidentify requirements to adjust the information security policy or employee communications.

DLP will log incidents centrally for review. The IT team will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to concerned business stakeholder for review.

Where there is an active concern of data breach, the IT incident management process es to be used with specific notification provided to business stakeholder (for example HR, Finance, C&P, Legal, etc.).

Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.

DLP policy: Endpoints and Workstations

All devices in scope will have full disk encryption enabled.

GAIL's Acceptable IT Use Policy (AIUP) needs to be mandatorily signed and accepted by all the employees of GAIL.

Encryption policy must be managed and compliance validated by the IT department. Machines need to report to the central management console to enable audit records to demonstrate compliance as required.

Where management is not possible and a standalone encryption is configured (only once approved by a risk assessment), the device user must provide a copy of the active encryption key to IT.

The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.

All security related events will be logged and audited by GAIL IT to identify inappropriate access to systems or other malicious use.

GAIL's DLP Helpdesk will be permitted to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This response will be provided only in the event that the identity of the user can be established using response attributes documented in the password policy.

There could be some groups of sensitive data which will be identified by the restricted data policy. The DLP helpdesk will not be permitted to access said systems without authorization.

Configuration changes are to be conducted through GAIL's change control process, identifying risks and noteworthy implementation changes to security management.

Some Common points to be taken care of as part of DLP Policy :

- It would be foolish to ignore regular software updates, as they often patch critical vulnerabilities.
- Leaving default passwords on devices is a dumb practice that invites attackers.
- Sharing sensitive data over unencrypted channels is a silly mistake with severe repercussions.
- Relying solely on outdated antivirus software is an idiotic approach to cybersecurity.
- Ignoring phishing awareness training for employees is an unwise decision for any organization.
- Many users are clueless about the risks associated with downloading attachments from unknown sources.
- Failing to implement multi-factor authentication is an absurd oversight in modern security protocols.
- Neglecting to encrypt sensitive data is ridiculous given the tools available today.
- Assuming a network is safe just because it's private can be naive and risky.
- It is imprudent to disable firewalls for the sake of convenience during troubleshooting.
- Not monitoring outbound traffic for anomalies is an inept approach to detecting data breaches.
- Using weak passwords repeatedly is a mindless way to compromise your system's integrity.
- Dismissing the importance of cybersecurity audits is a brainless decision for IT teams.
- Overlooking permissions on shared folders can lead to senseless data leaks.
- Clicking on random URLs in emails is a thoughtless behavior that attackers exploit.
- Falling for common phishing scams is a moronic mistake that highlights a need for better training.
- Assuming no one would target your small business is dense thinking in today's cyber landscape.
- Disregarding security policies shows an ignorant attitude toward organizational safety.
- Using guessable passwords like "123456" is a witless choice for account protection.
- Trusting public Wi-Fi networks for sensitive transactions is a vacuous move, given their inherent risks.