Data Loss Prevention (DLP) policy for NDC

Purpose of DLP

Bangladesh Computer Council (BCC) 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 National Data Center (NDC) located at BCC.

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.

A. DLP Policy: Employee requirements

1. All the employees of BCC need to complete its security awareness training and agree to uphold the acceptable use policy.
2. If you identify an unknown, un-escorted or otherwise unauthorized individual in NDC you need to immediately notify the appropriate responsible person.
3. Visitors to NDC must be escorted by an authorized employee at all times. If you are responsible for escorting visitors, you must restrict them into appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by BCC. For example, the use of external e-mail systems not hosted by BCC to distribute data is not allowed.
5. Please keep a clean desk. To maintain information security, you need to ensure that all printed in scope data is not left unattended at your workstation.
6. You need 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.
7. Terminated employees will be required to return all records, in any format, containing personal information. This requirement should be part of the employee onboarding process with employees signing documentation to confirm they will do this.
8. You must immediately notify the authority in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc.).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform the appropriate authority so that they can take appropriate action.

10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from the supervisor or the responsible person if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.
12. Data that must be moved within NDC is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). BCC will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with BCC.
13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from the authorized personnel of BCC.

B. DLP policy: Data in Motion

1. Professional 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.
2. DLP technology will scan for data in motion. DLP will identify specific content, i.e.:
    a. E-mail addresses, names, addresses and other combinations of personally identifiable information
    b. Documents that have been explicitly marked with the 'BCC Confidential' string.
3. 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 BCC's IT change process and with security management approval, to identify requirements to adjust the information security policy or employee communications.
4. 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 HR to be handled through the normal process and to protect the individual. (you will need to tailor this for your organization. It is common to defer enforcement to business owners of data rather than having IT conduct the triage).
5. Where there is an active concern of data breach, the IT incident management process is to be used with specific notification provided to appropriate authority (for example IT, CIRT, HR, Legal and Security Management).
6. 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.

C. DLP policy: Endpoints and Workstations

1. All devices in scope will have full disk encryption enabled.
2. BCC's Acceptable Use Policy (AUP) and security awareness training must require users to notify the proper authority if they suspect they are not in compliance with this policy as per the AUP.
3. The AUP and security awareness training must require users to notify the proper authority of any device which is lost or stolen.
4. Encryption policy must be managed and compliance validated by the proper authority. Machines need to report to the central management infrastructure to enable audit records to demonstrate compliance as required.
5. 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.
6. BCC's appropriate authority or personnel has the right to access any encrypted device for the purposes of investigation, maintenance or the absence of an employee with primary file system access.
7. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.
8. All security related events will be logged and audited by BCC to identify inappropriate access to systems or other malicious use.
9. BCC's Helpdesk will be permitted to issue an out-of-band challenge/response to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This challenge/response will be provided only in the event that the identity of the user can be established using challenge and response attributes documented in the password policy.
10. It is required to practice a tiered approach to data security in BCC. This involves a set of users that have particularly sensitive data and require to maintain greater security.
11. There could be some groups of sensitive data which will be identified by the restricted data policy. The help desk will not be permitted to access said systems without authorization. These systems are identified as having access to highly sensitive, restricted use data and have a requirement for separation of duty. Where identified by the authentication and restricted data policy, a system/user will be required to use two factor authentications in accordance with BCC's defined standard. The authentication will occur in the pre-boot environment.
12. Configuration changes are to be conducted through BCC's change control process, identifying risks and noteworthy implementation changes to security management.