SELCOM PAYTECH LTD
DATA LEAKAGE AND PREVENTION POLICY

Contents

1 Policy Statement

Selcom will establish specific requirements for protecting Data and Use of tools against unauthorized access and will effectively communicate the need for information and information system access control.

2 Purpose

Data loss prevention (DLP) is the practice of detecting and preventing confidential data from being "leaked" out of an organization's boundaries for unauthorized use. Data may be physically or logically removed from the organization either intentionally or unintentionally

3 Scope

The Scope of this policy and control is prevent any data leak on Selcom network whether its internal or external breach. Also caters for the controls in place to manage any such data loss that can damage company reputation or put's Selcom into risky business.

4. **Definition**:

Identify and classify your data. A well-developed, granular data classification scheme will enable your company to design and implement the proper controls for different types of data. A data inventory, linkingthe data classification scheme to specific data held within the IT infrastructure and with external parties, will help appropriately scope your DLP program.

5. Define Data Categories

Corporate Data	Transaction Data	Customer Data	Personal Data
Price/cost lists Target customer lists New designs Source code Formulas Process advantages Pending patents Intellectual property Unreleased merger/ acquisition plans and financial reports Legal documents Employee personal data	Bank payments B2B orders Vendor data Sales volumes Purchase power Revenue potential Sales projections Discount ratios	Customer list Contact details User preferences Product customer profile Payment status Contact history Account balances Purchase/transaction history Payment/contract terms Account No. PAN/Card No.	Full Name Birthday, birthplace Biometric data Genetic information Credit card numbers National identification number, passport numbers Driver’s license number, vehicle registration number Associated demographics Preferences

6. Reasons for Data Loss or Data Leakage

Root Cause of Data Loss	Data Category	Description
inappropriate access rights to applications with sensitive data	Customer data	A frustrated staff member used the standard data export procedures to export sensitive data and copied it to a CD.
Exploitation of weaknesses in a database's development environment	Personally, identifiable data	A database administrator with an understanding of test procedures could reverse engineer a sanitized process by referencing hidden tables

Breach of trust between developers	Transaction data	An experienced IT developer could reconstruct transaction data by gaining access to confidential data from an inexperienced developer unaware of the company’s access policies and restrictions
Unsupervised front office	Corporate data	A call center staff member provided screenshots of internal systems to fraudsters to help them reverse engineer an application.
Employee discontent	Corporate data	An employee leaving the company came in over a weekend prior to resigning on Monday, accessed the customer master file and exported it to an Excel file. This file was then emailed to the employee’s personal email account
Insider trading	Corporate data	An employee with access to prerelease financial information fed information to an external analyst, resulting in improper stock trades for both the employee and the analyst

7. Data Loss Prevention by Selcom

   a. **Internet access control:**

We use PSense FW which enables us to protect the data transmitted in and out of Selcom infrastructure. Currently we have Firewall and Router which has the facility for Rule Setting that enable to remove unwanted data or any such data that requires scrutiny

b. **Email Security:**
Selcom use G Suite Business edition DLP Facility for managing email content for inbound and outbound communication in regarding to company information. Gmail data loss prevention (DLP) lets you scan your organization's inbound and outbound email traffic for content, such as credit cardor Social Security numbers, and set up policy-based actions when this content is detected.
Available actions include sending the message to quarantine, rejecting the message, or modifyingthe message.

c. **Perimeter security**:
We are in process of devising a tool that will block all devices to transmit data via external mediumsuch as USB, CD or memory Cards. Using the device Lock mechanism software that enables to achieve the required objective

d. **Network monitoring:**
Monitor Network devices and data transmitted in and out of Selcom Server Room. Network Monitoring Tool such as Spiceworks and Open DNS are implemented to managed all Hardware/Software devices along with Managing Network and Bandwidth Monitoring for the trafficwhich is being sent and received

e. **Use of instant messaging:**
Only IM is allowed in the company which is Skype for business purpose only. Which is further monitored at Firewall level on the data transmission

f. **Remote access:**
Encrypted remote access, restrictions on use of remote access tools to prevent data leakage to non-corporate assets. All Remote access to Selcom Network is assigned to 2 individualswho can access the data during emergency or any such disaster

g. **Data collection and exchange with third parties:**
A standard SLA is signed by any partner and thus includes the aspect of data prevention or dataloss during the term defined. Selcom emphasizes on policy to be implemented by partners to secure data end to end.

h. **Use of test data:**
Do not use or copy sensitive data into non-production systems. Sanitize data before moving into test systems when possible. Selcom has test and production facility in place. All systems which arefor test purpose are connect to the test environment and is confirmed during such test

i. **Data Encryption:**
All User HDD are encrypted by default using Windows BIT Locker which is part of Windows 8 andonwards

8. Risk Assessment and DLP

Selcom is an IT based company and security risks are the main factor to be analyzed and see what preventions can be implanted during the life cycle of a product or service.

Following Risks and Mitigation Process are in process to be in place in case a DLP is not implemented asrequired

Risk	**Impact**	**Mitigation**
Improperly tuned network DLP modules	Disruption of business processes Lost time and revenue Damage to customer or business partner relationships Loss of business stakeholder support	Proper tuning and testing of the DLP system should occur before enabling actual blocking of content. Enabling the system in monitor-only mode will allow for tuning and provide the opportunity to alert users to out-of-compliance processes and activities so they may plan accordingly. Involving the appropriate business and IT stakeholders in the planning and monitoring stages will help ensure that disruptions to processes will be anticipated and mitigated. Finally, establish some means of accessibility in the event there is critical content being blocked during off-hours when the team managing the DLP solution is not available.
Improperly sized network DLP module	Missed or dropped network packets allowing data to pass uninspected	Ensuring that the size of the DLP module is appropriate for network traffic is a critical design consideration? However, it is just as important to monitor the DLP network modules to ensure that network traffic does not increase over time to a point that renders the module ineffective.
Excessive reporting and false positives	Wasted staff time Missing valid threats Tendency to ignore logs over time	Similar to an improperly configured intrusion detection system (IDS), DLP solutions may register significant amounts of false positives, which overwhelm staff and can obscure valid hits. Avoid excessive use of template patterns or “black box” solutions that allow for little customization. The greatest feature of a DLP solution is the

		ability to customize rules or templates to specific organizational data patterns. It is also important that the system be rolled out in phases, focusing on the highest risk areas first. Trying to monitor too many data patterns or enabling too many detection points early on can quickly overwhelm resources.
Conflicts with software or system performance	System down time Performance degradation Breaking of DLP or other controls or processes	DLP systems, particularly crawlers and end-point agents, can conflict with other system software and performance. Allowances must be made for ample planning and testing before deployment. Ideally, a permanent testing and staging environment should be available. Check with the vendor for known conflicts. Ensure that crawlers are properly configured and tuned, and that their operation is scheduled in such a way as to avoid peak system processing windows. When avoidable, end-point scans should not be scheduled for peak work hours or when systems are remotely connected. Also ensure that all patches and upgrades are tested within the test environment prior to deployment to production
Changes in processes or IT infrastructure rendering DLP controls ineffective	Reduction of DLP effectiveness due to circumvention of DLP controls	The DLP system administrator or a representative should be involved in change control processes to ensure that changes made do not circumvent or otherwise degrade DLP capabilities. In addition, the enterprise should be well prepared for changes associated with DLP to reduce risk of intentional bypassing of the DLP system in the name of efficiency.
Improperly placed DLP network modules	Missed or uninspected data streams	it is important to ensure proper placement of DLP network modules. Ensure that accurate network maps are available, and that the modules are placed at the outermost egress point for data flows the enterprise wishes to monitor

Undetected failure of DLP modules	Data not inspected due to partial or complete module failure	DLP modules can fail, but do not always report their state to the console. It is important to periodically test to ensure that modules and their associated filters are performing as expected.
Improperly configured or incomplete directory services	Inability to trace violations to the appropriate end users	The directory service is the key connection between a network address and an actual user, and most enterprises will want to have this process in place as opposed to manual discovery of this information, which can be time consuming and is not always possible. Enterprises that lack or have incomplete directory services should consider addressing this gap prior to implementing a DLP solution

9. Policy Compliance

If any user is found to have breached this policy, they may be subject to Selcom's disciplinary procedure. If a criminal offence has been committed further action may be taken to assist in theprosecution of the offender(s).The Policy of breaching is maintained by HR/Admin Department.

10. Policy Governance

The following table identifies who within Selcom is Accountable, Responsible, Informed or Consultedwith regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation oramendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	CEO, Compliance Officer and Head of Technology and Software Department

Accountable	All HOD are accountable on their individual Staff access
Consulted	Internal Compliance and Technology and Software Department
Informed	All Staff Internal and External

11. Review and Revision

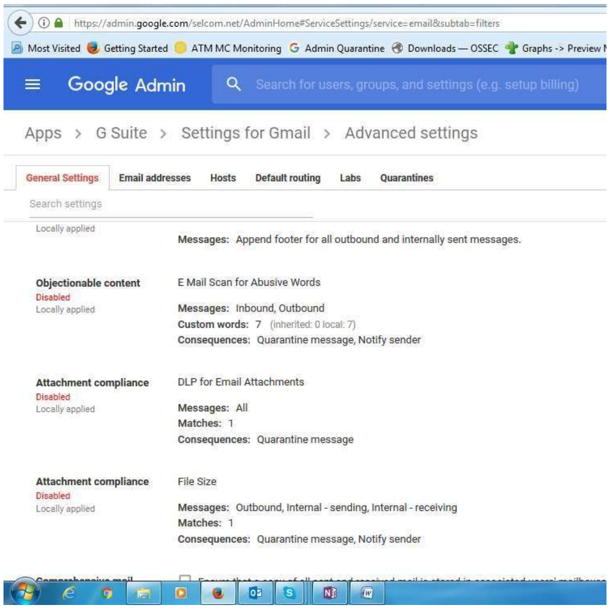
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.Policy review will be undertaken by IT Compliance Officer and Technology and Software Development Department.

12. Document Control

Date	Version	Requester	Tech. Writer	Change/Review
21-06-2017	V1.0	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
30--08-2017	V1.1	Deloitte/SCB	Mohammedjawaad Kassam *Additional Content for Appendix showing DLP Settings using G-Suite* *Adding Document Control and Version Control*	Sarah Mohammed

13. Appendix

DLP using G-Suite from Google Business


https://admin.google.com/selcom.net/AdminHome#ServiceSettings/service=email&subtab=filters
Most Visited
Getting Started
ATM MC Monitoring
Admin Quarantine
Downloads — OSSEC
Graphs -> Preview
Google Admin
Search for users, groups, and settings (e.g. setup billing)
Apps > G Suite > Settings for Gmail > Advanced settings
General Settings
Email addresses
Hosts
Default routing
Labs
Quarantines
Search settings

Locally applied

Messages: Append footer for all outbound and internally sent messages.

Objectionable content
Disabled
Locally applied

E Mail Scan for Abusive Words

Messages: Inbound, Outbound
Custom words: 7 (inherited: 0 local: 7)
Consequences: Quarantine message, Notify sender

Attachment compliance
Disabled
Locally applied

DLP for Email Attachments

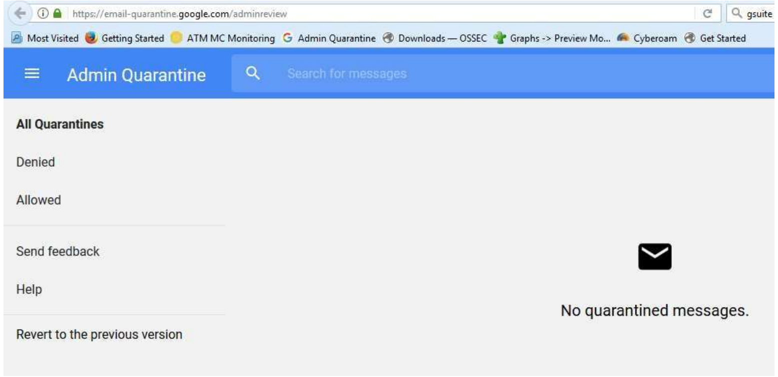
Messages: All
Matches: 1
Consequences: Quarantine message

Attachment compliance
Disabled
Locally applied

File Size

Messages: Outbound, Internal - sending, Internal - receiving
Matches: 1
Consequences: Quarantine message, Notify sender

Messages to be released or blocked incase it does not meet the policy set using DLP



No quarantined messages.