Data (Privacy) Protection Policy
Incorporating personally identifiable information (PII)

Table of Contents

(1) PURPOSE

Due to its very nature, sensitive data must be protected from unauthorized access or disclosure. The purpose of this Policy is to establish an Information Protection program within Nuss that offers compliance with federal and state laws and regulations, as well as protects data that if compromised either through availability, confidentiality, or integrity, could cause significant financial or reputational damage to the company.

(2) SCOPE

This policy pertains to all data, applications, and resources that are owned, managed, and/or administered within the scope of the Nuss information systems. This includes data maintained electronically as well as information available in hard copy (paper) format.

(3) GENERAL

Nuss is committed to protecting specific types of information, which, if disclosed, could reasonably be expected to result in harm to the company, an identifiable individual, or a third party. In general, sensitive information is information that contains an element of confidentiality. It includes information that is exempt from disclosure by the Privacy Act and information whose disclosure is governed by the Privacy Act of 2012. Sensitive information requires a higher level of protection from loss, misuse, and unauthorized access or modification. Failure to protect sensitive information may cause Nuss to be in violation of the law or may result in avoidable costs or damage to its reputation.
This subset of information, includes personal information, business records, as well as client details, labour relations and other kinds of information which for the purposes of this policy, all need to be protected.
Specifically, in recent years, the increase in the incidence of identity fraud has focused attention on protecting the privacy of individuals by both commercial businesses and government agencies. In the role as an employer, as well as in support of its mission, Nuss collects and maintains information about employees and other individuals as well as information obtained from other sources including vendors, business clients and their transferees. Accordingly, the Corporation has a responsibility to protect this personally identifiable information (PII).

(4) RISKS

As with all policies and procedures, initially risks are identified that require remediation, causing the need for a documented approach. The following risks were determined, and are addressed through this policy.

- As the world has become more reliant on technology, high-tech criminals have also adapted, becoming more and more sophisticated and can exploit human error and weak security controls to steal trade secrets, payment card data, employee and customer information, and other personal information;
- Hackers not only rob a company of data, they impugn its integrity, breach its trust with clients and customers, and damage its brand and reputation;
- Well-meaning employees may lack the tools and training to protect high-risk data.

(5) DEFINITIONS

Confidential Information: The term "confidential information" applies broadly to information for which unauthorized access to or disclosure could result in an adverse effect. To address this risk, some degree of protection or access restriction may be warranted.

Restricted Data: Restricted data is a specific category of confidential information.
Restricted data is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.
Personal identity information (PII) is the electronic manifestation of an individual first name or first initial, and last name, in combination with one or more of the following (this is not a complete list):

- Social Security Number (SSN)

- Driver's licence number, or State-Issued ID card #
- Account number, credit or debit card number
- Medical information
- Health insurance information

(6) POLICY

In order to protect sensitive information, it is the policy of Nuss to:

- Collect and retain sensitive information only when it is necessary to satisfy a Nuss business requirement, and only as long as necessary;
- Know where sensitive information is by identifying its existence in both electronic and paper formats, and assign ownership;
- Label removable electronic media (e.g., diskettes, CD/DVD, USB flash drives) and paper reports (on the cover page and/or in the footer section) as containing sensitive.
- Safeguard sensitive information from unauthorized access. Only those individuals who have a legitimate need to access sensitive information in the performance of their duties shall be provided access;
- Store sensitive electronic information only on corporate information technology (IT) equipment;

- Store paper copies in corporate facilities (e.g., locked drawers, file cabinets, and file rooms) whenever possible;

- Sensitive information shall not be removed from the workplace without prior management approval, and if it must be removed, it shall be kept secured at all times. Whether in electronic or paper format, it shall not be left unattended unless properly physically secured;

- Encrypt sensitive information stored on end-user IT equipment (e.g., laptop and desktop computers) as well as on removable media (e.g., diskettes, CD/DVD, USB flash drives);

- Remotely access sensitive information stored in electronic format only across a secure connection, such as via remote access services;

- Do not use actual sensitive data in test or development systems, or for training purposes. Sanitize or create appropriate data for those situations. If actual restricted data must be used, it must be protected appropriately.

- Send sensitive information electronically only when required, and over a secure link whenever possible. If a secure link is not available, such as when sending E-mail containing sensitive information outside Nuss via the Internet, the E-mail message and/or its contents must only be sent to a known address and with details included only on a ‘need to know basis’. Such emails to be followed up to ensure confirmation of receipt by the receipient.

- Ship sensitive information by postal service or commercial carrier only when required. The shipment shall be tracked and followed up on in a timely manner to ensure that it arrives intact at its destination;

- Restricted data must be destroyed or completely and securely removed from computers and electronic media (including backups) before disposal, re-use or re-assignment.

- Properly dispose of electronic media and paper documents containing sensitive information when they are no longer needed. Electronic media and paper documents shall not be discarded intact in a rubbish bin. Paper documents shall be shred (or placed in a shred bin provided by Nuss) and electronic storage media shall be destroyed (or placed in an electronic media console provided by Nuss);

- Require all employees and contractors to complete annual security and privacy awareness training;

- Truncate, de-identify or redact restricted data that you must retain whenever possible, or when responding to an incident.

In the event that sensitive data is suspected or known to be lost or otherwise compromised, whether in electronic or paper format, report the situation immediately to the Nuss Privacy Officer. Also notify your supervisor/manager at the earliest available opportunity.

(7) ROLES

The following subsections describe key roles and specific responsibilities of the individuals involved in ensuring compliance with this Policy.

Nuss employees are responsible for reviewing and understanding this policy and the related procedures. Senior Management and the Privacy Officer are responsible for disseminating the policy and Procedures to employees, making the Policy and Procedures widely available, and developing the necessary tools, trainings and forms to support the Procedures.

This policy and the related Procedures shall be maintained and updated on an ongoing basis by the Privacy Officer

(8) VIOLATIONS

Any Nuss system user found to have violated any policy, procedure, standard or guideline may be subject to disciplinary action, up to and including termination of employment. Violators of state, Federal, and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Specifically, a violation of this policy will facilitate an incident report being filed, and additional actions being taken to report, and prevent the violation from occurring in the future.

(9) EXCEPTIONS

While every exception to a policy or standard potentially weakens protection mechanisms for Nuss information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available. All exceptions must be documented and approved prior to implementation.

(10) APPENDICES

RECORDS

Updates to the policy will be announced to employees via management updates, icon in computer or email announcement.