Data Protection and Security Policy

Context and Overview

Key Details

- Policy prepared by: Technology Operating Committee
- Approved by management on: 10/5/2021
- Policy became operational on: 10/5/2021
- Next review date: 10/18/2023

Introduction

Raise from Gravyty ("Gravyty", "the company") needs to gather and use certain information to enable the proprietary algorithms of the system to function and to display information to enable the usability of the system. Some of this data is personal, sensitive, and/or confidential, including, but not limited to, personally identifiable information (including names, postal and email addresses, and telephone numbers), past emails, donor transaction data, prospects, employee information, projections, and targets that are collected on a recurring basis ("Protected Data").

This policy describes how Protected Data shall be collected, handled, and stored to comply with applicable law and best practices.

Objective

Information and data security is defined as the protection (or preservation) of:

- **Confidentiality**. Ensuring that information is accessible only to those persons authorized to have access.
- **Integrity**. Safeguarding the accuracy and completeness of information and information processing methods.

- **Availability**. Ensuring that authorized users have access to information and information systems in a timely manner, when they are needed.

This policy ensures that the company:

- Complies with data protection law and follows best practices.
- Protects the rights of staff, customers, and partners.
- Is open about how it stores and processes data to the extent practicable in balancing concerns about disclosing protective technologies or techniques.
- Protects itself from the risks of a data breach.

People, Risks, and Responsibilities

Policy Scope

This policy applies to the protection of Protected Data by and on:

- The head office and all branches of the company.
- All staff and volunteers of the company.
- All contractors, suppliers, and other people working on behalf of the company.
- Any devices, regardless of ownership and including equipment privately owned by staff (e.g. laptops, tablets, smart phones, MP3 players, USB storage devices, etc.), but only with respect to the ways in which those device connect to, access, or store Protected Data and the activities they perform with that Protected Data.

Data Protection Risks

This policy helps to protect the company and our clients from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the company has responsibility for ensuring Protected Data is collected, stored, and handled appropriately.

Each team that handles Protected Data must ensure that it is stored, handled, and processed consistent with this policy.

However, these people have key areas of responsibility:

- The **Technology Operating Committee (TOC)** is responsible for:
    - Keeping the company updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from those covered by this policy.
    - Dealing with requests from individuals to see the data that the company holds about them.
    - Checking and approving contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services, and equipment used for storing and/or processing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party service the company is considering using to store or process data for compliance with this policy (for instance, cloud computing services).
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives comply with this policy.

Web Application Guidelines

Web applications are subject to security assessments based on the following criteria:

- **New or Major Releases** will be subject to a documented Quality Assurance assessment prior to the approval of the change and/or release into the production environment.
- **Third-Party Applications** will be subject to review by the TOC prior to its code being part of the existing code base or used on any of our development devices.
- **Patch Releases** will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

Identification and Authentication Guidelines

- The only people able to access Protected Data are those who **need it for their work**.
- Two-factor authentication is required for personnel who need to access Protected Data.
- Protected Data **must not be shared informally**. When access to confidential information is required, employees can request it from their direct managers. **The company will provide real-time and pre-recorded training** to all employees to help them understand their responsibilities when handling Protected Data.
- Employees should keep all Protected Data secure, by taking sensible precautions and following the guidelines below.
- **Strong passwords must be used** and they should never be shared. Password requirements are:
    - Passwords must have at least twelve (12) characters.
    - Passwords can't contain the username, email address, or parts of the user's full name, such as his or her first name (spelled forward or backward).
    - Passwords cannot be the same as your last 3 passwords
    - Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
- Protected Data **must not be disclosed** to unauthorized people, either within the company or externally.
- Protected Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of in accordance with federal, state, and local law.
- Employees **should request help** from their direct manager or the TOC if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where Protected Data must be stored. Questions about storing Protected Data safely can be directed to the TOC.

When Protected Data is **recorded on paper**, it should be kept in a secure place where unauthorized people cannot see and access it in accordance with the following best practices:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer or face-up on a desk.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts in accordance with the following best practices:

- Protected Data must be **protected by strong passwords** that are changed every 90 days and never shared between employees.
- If Protected Data is **stored on removable media** (like a CD, DVD, USB drive), these must be kept locked away securely when not being used. Encryption is required for Protected Data stored on removable media.
- Protected Data must only be stored on **designated drives and servers**, and should only be uploaded to **approved cloud computing services.**
- Protected Data backups should be tested regularly and kept in a secure location behind a firewall.
- Protected Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing Protected Data must be protected by **approved security software and a firewall**. Current protections include:
    - Transport Layer Security (TLS) 1.2 or later
    - Encrypted database connections; Secure Shell (SSH)
    - Data Center Accreditations (Amazon AWS & Heroku)
        - ISO 27001
        - SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
        - PCI Level 1
        - FISMA Moderate
        - Sarbanes-Oxley (SOX)
    - Host-based Firewalls
    - DDoS Mitigation including TCP cookies
    - Spoofing and Sniffing protections (hypervisor)
    - Port scanning
    - Automated Services For
        - Vulnerability management (updates, fixes, configuration)
        - Disaster recovery
        - Media Sanitization & Data Destruction immediately after upload/import
        - Logging, Error Reporting, Intrusion Monitoring

Protected Data Use

Protected Data is of no value to the organization unless the business can make use of it. However, it is when Protected Data is accessed and used that it can be at the greatest risk of loss, corruption or theft. The following best practices must be followed when using Protected Data

- When working with Protected Data, employees must **lock the screens of their computers** when left unattended.

- Protected Data **must not be shared informally.**
- Protected Data must be **encrypted before being transferred electronically** over unsecure mediums.
- Protected Data should **never be transferred outside of the United States.**
- Employees **should not save copies of Protected Data to their own computers.** Always access and update the central copy of any data.

Data Accuracy

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Protected Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- The company will make it **easy for data subjects to update the information** the company holds.
- Protected Data should be **updated as inaccuracies are discovered.**

Data Breach Procedure

Where a data breach is known to have occurred (or is suspected) any member of the Gravyty staff who becomes aware of this must, within 1 hour, alert a member of the TOC or other member of the Executive Team if the TOC is not available.

The information that should be provided (if known) at this point includes:

A. When the breach occurred (time and date)
B. Description of the breach (type of personal information involved)
C. Cause of the breach (if known) otherwise how it was discovered
D. Which system(s), if any, are affected?
E. Which clients/users/staff are involved?
F. Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

Once notified of the information above, the Member of the Executive team must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgment as to its severity. The Executive team will then relay this information to the Privacy Response Team, which includes the Technology Operating Committee.

The following steps may be undertaken by the Response Team, within 4 hours of being convened (as appropriate):

- Immediate containment of the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of personal information, ceasing unauthorized access, shutting down or isolating the affected system.

- Email and/or contact via phone the primary client point(s) of contact to inform them of the information surrounding the breach and remediation actions.
- Evaluating the risks associated with the breach, including collecting and documenting all available evidence of the breach
- Engage in independent cyber security or forensic export as appropriate and deemed necessary by the TOC

To date, no data breaches have been observed or suspected.

Return / Destruction of Data

Upon the written request of the client, as applicable and in accordance with law, within a reasonable time period after termination of their Agreement, for any reason, the company shall return or destroy (as specified by the client) all client data and indexing information received from the client, or created or received by the company on behalf of the client.

Destruction of client data will be conducted in accordance with standard industry practices, including, but not limited to, secure digital shredding. Upon request, the company shall provide proof or certification of destruction of data to the client.

Disclosing Data

The company will disclose Protected Data to governmental authorities as required by law, and potentially without the consent of the data subject, only after the TOC ensures the request is legitimate and seeks assistance from management, the company's legal advisers, and the client.

Providing Information

The company aims to ensure that users are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to usage is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]

Policy Compliance

The company will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the TOC.

The TOC must approve any exception to the policy in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.