Document details:

Title	Data Breach Policy Statement
Document ID	EXT005
Version number	2.02/1222
Status	Published
Published date (web)	01/23
Author	Rick Dye
Approved by	Board of Directors
Review date	12/23
Review frequency	Annual

Revisions:

Version	Date	Description	Revision
1.01	01/22	Original document	Original copy
2.01/1222	01/23	Updated	All details by Clover
2.02/1222	09/23	Updated	Added page 1 document details

Dependencies and related policies or process:

Document	Location
Data Protection Policy	Data-Protection-Policy.pdf (grillatech.com)
Data Breach Process	Process powerpoint presentation

Data Breach Policy Statement

This is the statement of general policy and arrangements for:

Grillatech Limited

Overall and final responsibility for data breach:

Services Director

Grillatech is totally committed to the principles and practice of a breach response process.

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritisation of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicised and made easily available to all personnel whose duties involve data privacy and security protection.

Grillatech ‘s intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Grillatech’s established culture of openness, trust and integrity should respond to such activity. Grillatech is committed to protecting Grillatech's employees, contractors, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1. Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Grillatech’s protected data or sensitive data has occurred must immediately provide a description of what occurred via e-mail to info@grillatech.com, or by calling 0333 772 0875, or through the use of the contact web page at https://Grillatech.com/. This e-mail address, phone number, and web page are monitored by Grillatech’s administrator, office manager and management team. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2. Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of Grillatech employees. Any agreements with vendors will contain language similar that protects their information.

3. Policy Confirmed theft, data breach or exposure of Grillatech protected or sensitive data

As soon as a theft, data breach or exposure containing Grillatech protected data or sensitive data is identified, the process of removing all access to that resource will begin.

The Managing Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT/Technical team
- Finance (if applicable)
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Managing Director

Confirmed theft, breach or exposure of Grillatech data

The Managing Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyse the breach or exposure to determine the root cause.

4. Work with Forensic Investigators

As provided by Grillatech insurance, the insurer may need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organisations impacted; and analyse the breach or exposure to determine the root cause.

5. Develop a communication plan

Work with communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

6. Ownership and Responsibilities

Roles & Responsibilities:

- Information Security Administrator is that member of the Grillatech community, designated by the Managing Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the Grillatech community to the extent they have authorised access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives; Communications; Legal; Management; Financial Services; Human Resources.

7. Enforcement

Any Grillatech personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

8. Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data;

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered;

Protected data - See PII;

Information Resource - The data and information assets of an organisation, department or unit.
Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset;

Sensitive data - Data that is encrypted or in plain text and contains PII data. See PII above.