Information Security & Data Protection Policy

Version 1

VANQUISH TECH

Our framework for managing data protection and security in our organization typically includes policies, procedures, and controls to protect sensitive information from unauthorized access, use, disclosure, or destruction. This framework is typically overseen by a engineer for managing data protection and security and reported directly to our cloud and services director.

Here is an overview of what the framework and reporting in more detail:

1. Policies and procedures:

The framework includes policies and procedures for data protection and security that outline the company's approach to protecting sensitive information. These policies might include:

- Access control: guidelines for controlling access to sensitive information, including the use of strong passwords, two-factor authentication, and restricted access to certain systems or data.
- Data classification: a system for categorizing data according to its level of sensitivity and specifying how each category of data should be protected.
- Incident response: procedures for responding to security incidents, including who to contact, what to do, and how to recover from a breach.
- Third-party risk management: policies for managing the risks associated with third-party vendors, contractors, or other partners who have access to the company's data.

2. Controls:

We value integrity and hold ourselves accountable for our actions. We promote a culture of transparency, trust, and fairness in all our interactions, both within the organization and with external stakeholders.

- Technical controls: such as firewalls, intrusion detection systems, encryption, and anti-virus software.
- Administrative controls: such as employee training, security awareness programs, and access control policies.
- Physical controls: such as locks, access control systems, and security cameras.

3. Oversight groups/ steering groups:

Our engineers are responsible for ensuring that data protection and security policies are being followed through-out the organization and are reported to the cloud & services director.

4. Information risk reporting:

We Information risk would be reported to SMT/board level in several ways, such as:

- **Regular reports from the data protection and security team:** These reports would cover the current state of data protection and security within the company, any significant incidents or breaches that have occurred, and any upcoming initiatives or projects related to data protection and security.

- **Dashboards or metrics:** We report on key security indicators, such as the number of incidents or breaches, the number of vulnerabilities identified and remediated, and the status of compliance with relevant GDPR regulations. Ad-hoc reports: The data protection and security team also prepare ad-hoc reports for senior management or the Board as needed, such as in response to a major incident or to provide updates on a specific project. The goal of reporting is to ensure that senior management and the Board are fully informed about the company's data protection and security practices, and that they have the information they need to make informed decisions about risk management and strategic planning.

REGISTERED

ISO Certified

ISO 9001 ISO 27001 ISO 22301 ISO 14001

CYBER ESSENTIALS

CERTIFIED

LONDON - HEAD OFFICE (UNITED KINGDOM)
Salisbury House
29 Finsbury Circus
+44 (0) 20 3141 2910
UK Reg # 7843165
VAT # GB 124 406 447

FLORIDA(USA)
516 S Dixie Hwy #214
West Palm Beach
FL 33401
+1 561 954 4790

DUBLIN (IRELAND)
6 Fern Road, Dublin
D18 FP98
+353 (0) 1584 5910

VANQUISH TECH