# Information Security Policy

Classified: External

Organisation Issue No: 3

Organisation Issue Date: 22/5/2022

Document Owner: [Information Security Manager](#)

Reference: ISMS DOC 5.2

The management of IDDQD Limited are committed to preserving the confidentiality, integrity and availability of all the information assets, throughout the organisation. By doing so, IDDQD Limited will preserve its competitive edge, profitability, regulatory and contractual compliance and brand image. Privacy and information security requirements will continue to be aligned with IDDQD Limited's goals. The ISMS is intended to document a mechanism for information sharing, digital operations, and for reducing information and privacy-related risks to acceptable levels.

IDDQD Limited is committed to ensuring compliance with all applicable legislative, regulatory and contractual requirements, including all applicable PII protection legislation.

IDDQD Limited's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information and privacy-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and [Risk Treatment Plan](#) identify how information and privacy-related risks are controlled.

The [MD](#) is responsible for the management and maintenance of the [risk treatment plan](#). Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity, data backup procedures, avoidance of viruses and hackers, access control, and information security and privacy incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Information Security Manual and are supported by specific documented policies and procedures.

IDDQD Limited aims to achieve specific, defined information security and privacy objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the [risk treatment plan](#). IDDQD Limited's Information Security and Privacy Objectives and Planning Procedure detail how the company identifies, manages and tracks key objectives within the context of the organisation.

All [Staff](#) of IDDQD Limited and relevant external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All [Staff](#), and certain external parties, will receive appropriate training. The consequences of breaching the information security and privacy policies are set out in IDDQD Limited's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

IDDQD has established a [management team](#) chaired by the [MD](#) to support the ISMS framework and periodically review the security policy.

IDDQD Limited is committed to achieving certification of its ISMS to ISO 27001:2013.

This policy will be reviewed to respond to any changes in the risk assessment or [risk treatment plan](#) and at least annually.

In this policy, 'information security' is defined as:

# Preserving

This means that all [Staff](#) any external parties have responsibilities (defined in job descriptions or contracts) to preserve information security and privacy, to report breaches and to act in accordance with the ISMS. All [Staff](#) will receive information security and privacy awareness training, and more specialised [Staff](#) will receive appropriately specialised training.

# the confidentiality,

This involves ensuring that information is only accessible to those authorised to access it; preventing deliberate or accidental unauthorised access to IDDQD Limited's information and proprietary knowledge and its systems including servers, shared storage and code repositories.

# integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and requires preventing deliberate or accidental, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for client data, addressing data, shared storage, code repositories and data backup plans along with security and privacy incident reporting. IDDQD Limited must comply with all relevant data and privacy-related legislation in those jurisdictions within which it operates.

# and availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. Networks must be resilient and IDDQD Limited must be able to detect and respond rapidly to incidents that threaten the availability of assets, systems and information. There must be appropriate business continuity plans.

# of the physical (assets)

The physical assets of IDDQD Limited, including, but not limited to, computer hardware and physical data files.

# and information assets

The information assets include information (whether PII or otherwise) printed, transmitted by post, or spoken in conversation, stored on computers and other digital media.

# of IDDQD Limited.

IDDQD Limited and such partners that are part of the integrated network and have signed up to our information security and privacy policy and have accepted our ISMS.

The ISMS is the information security management system, of which this policy, the Information Security Manual and other supporting and related documentation are a part, and which has been designed in accordance with the specifications contained in ISO 27001:2013.

A security breach is any incident or activity that causes, or may cause, a break down in the confidentiality, integrity or availability of the physical or electronic information assets of IDDQD Limited.

A privacy breach is any incident or activity that causes, or may cause, a break down in the confidentiality, integrity or availability of the PII assets of IDDQD Limited.