Information Security Roles and Responsibilities Policy

Policy Owner: Neil Cameron

Effective Date: 1 May 2023

Statement of Policy

Make and Grow ltd is committed to conducting business in compliance with all applicable laws, regulations, and company policies. Make and Grow ltd has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy and associated guidance establish the roles and responsibilities within Make and Grow ltd, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Applicability

This policy is applicable to all Make and Grow ltd infrastructure, network segments, systems, and employees and contractors who provide security and IT functions.

Audience

The audience for this policy includes all Make and Grow ltd employees and contractors who are involved with the Information Security Program. Awareness of this policy applies for all other agents of Make and Grow ltd with access to Make and Grow ltd information and infrastructure. This includes, but is not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as "Make and Grow ltd community".

Roles and Responsibilities

Roles	Responsibilities
Board of Directors	• Oversight of Cyber-Risk and internal control for information security, privacy and compliance • Consults with Executive Leadership to understand Make and Grow ltd IT mission and risks and provides guidance to align business, IT, and security objectives

The Founders	• Approves Capital Expenditures for Information Security and Privacy programs and initiatives • Oversight over the execution of the information security and Privacy risk management program and risk treatments • Communication Path to Make and Grow ltd Board of Directors • Aligns Information Security and Privacy Policy and Posture based on Make and Grow ltd's mission, strategic objectives and risk appetite
CTO	• Oversight over the implementation of information security controls for infrastructure and IT processes • Responsible for the design, development, implementation, operation, maintenance and monitoring of IT security controls • Ensures IT puts into practice the Information Security Framework • Responsible for conducting IT risk assessments, documenting identified threats and maintaining risk register • Communicates information security risks to executive leadership • Reports information security risks annually to Make and Grow ltd's leadership and gains approvals to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Works with applicable executive leadership to establish an information security framework and awareness program • Serve as liaison to the Board of Directors, Law Enforcement, Internal Audit and General Counsel • Oversight over Identity Management and Access Control processes
Engineering Lead	• Oversight over information security in the software development process • Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls • Responsible for oversight over policy development related to systems and software under their control • Responsible for implementing risk management in the development process aligned with company goals
The Founders	• Responsible for compliance with the company's contractual commitments • Responsible for maintaining compliance with relevant data privacy and information security laws and regulations (e.g. GDPR, CCPA) • Responsible for adherence to company adopted information security and data privacy standards and frameworks including SOC 2, ISO 27001 and Microsoft Supplier Data Protection Requirements (DPR)
Customer Success Lead	• Oversight and implementation, operation and monitoring of information security tools and processes in customer production environments • Execution of customer data retention and deletion processes in accordance with company policy and customer requirements

Systems Owners	• Maintain the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with Make and Grow ltd policies on information security and privacy • Approval of technical access and change requests for non-standard access to systems under their control
Make and Grow ltd Employees, Contractors, temporary workers, etc.	• Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize Make and Grow ltd's exposure to contractual and regulatory liability • Adhering to company policies and standards of conduct • Reporting incidents and observed anomalies or weaknesses
The Founders	• Ensuring employees and contractors are qualified and competent for their roles • Ensuring appropriate testing and background checks are completed • Ensuring that employees and relevant contractors are presented with company policies and the Code of Conduct (CoC) • Ensuring that employee performance and adherence the CoC is periodically evaluated • Ensuring that employees receive appropriate security training
The Founders	• Responsible for oversight over third-party risk management process • Responsible for review of vendor service contracts

Policy Compliance

The CTO will measure the compliance to this policy through various methods, including, but not limited to—reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the CTO in advance. Non-compliance will be addressed with management and Human Resources and can result in disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1	1 May 2023	First version	Neil Cameron	Jonny Burch