QACA IT Governance Policy

IT Governance Policy	QACA-P-07-Rev00	Date: 17/10/2023

Contents

Introduction

Quality Austria Central Asia endeavors to an ever-evolving digital landscape, and safeguarding our cyber domain is vital. As a leading cyber security firm in India, this IT Policy serves as a comprehensive guide to protect our systems and data. Emphasizing collaboration between IT, HR, Admin, Operations and Finance teams, we foster a security-first culture to counter evolving cyber threats. Together, we fortify our digital fortitude, navigating the cyber frontier with resilience and unwavering commitment. Information is a vital asset, ours and our clients, and we have a duty to protect all such information.

Purpose

The purpose of this IT Policy is to establish guidelines and best practices for the secure and efficient use of information technology resources within the organization. The policy aims to protect the confidentiality, integrity, and availability of company data and systems, as well as comply with relevant cybersecurity regulations in India. This policy is a high-level document and is supplemented by additional policies, processes, standards, and procedure documents, which provide further details to specific controls.

Scope

This policy applies to Quality Austria Central Asia and all Employees, Contractors, and staff deputed by any contracted agency, hereinafter referred as staff. While the approach shall be mainly in the area under our direct business, we would also work towards influencing our suppliers and partners to undertake work that improves the quality of life. An Information Asset is any information or information system which is sensitive, confidential or has value to Quality Austria Central Asia, including third party information processed by it and its staff.

Objectives

1. To protect the confidentiality, integrity and availability of Information Assets
2. To provide information, without interruption as and when required by the users, and reduce the risk of information security breaches.
3. To provide assurance to clients of Quality Austria Central Asia that their information is secure.
4. To increase awareness of all staff and to instill appropriate behavious to protect information and data.

Definitions

Cybersecurity: Cybersecurity is an activity or process of protecting sensitive information and critical systems from internet threats and attacks.

Cloud computing: Cloud computing refers to delivering various services through the internet, including servers, networking, data storage, analytics, and software.

Cloud computing: Encryption is a process of securing data through encoding that gives access to the information through a specific key.

Firewall: A firewall is a defensive technology that secures your computer from attacks and threats.

IP Address: IP stands for Internet Protocol. An IP Address is a unique home address for your computer identifiable when communicating over a network.

Software: Software is an application used by a company for running internal operations and serving customers. Business software may include Enterprise Resource Planning (ERP), web servers, operating systems (OS), Customer Relationship Management (CRM), and productivity applications. For example, there is monday.com CRM that offers a range of software solutions.

Hardware: Hardware refers to the physical component of IT infrastructure and consists of all necessary elements in supporting the basic functioning of a device. Hardware includes storage and data centers, hubs and routers, and equipment such as cabling, power, and housing.

Network: A network is a collection of servers, computers, mainframes, peripherals, and other device connections necessary in ensuring security, network enablement, firewall, and internet connectivity. A network is also responsible for giving access to stored and transferred data through strictly controlled access points.

SaaS: Software as a Service (SaaS) is a method of software delivery that involves a subscription to an external provider.

IT Governance: Information technology governance refers to the leadership, structure, and process that ensures an organization's IT can sustain and support business strategies and objectives.

Back up: A backup is a virtual or physical copy of data that helps recover it if it is lost or deleted. It is one component of a data loss prevention plan.

Sub Policies

IT Hardware Policy

All hardware to be of approved make as laid down by IT department. Use of unapproved hardware is prohibited. Use of unapproved hardware is prohibited. Replacement of any hardware will require prior approval from the IT department. Request for all hardware will be the responsibility of HR Head / Circle Head. Asset Management of all hardware will be maintained by the IT department and is shared with Admin and Finance. Hardware includes all servers, desktops, laptops, company issued mobiles, tablets, printers, switches, routers etc.

IT Software Policy

Only authorized and licensed software may be installed on company devices, no software will be downloaded without approval from the IT department. Regular patches and updates would be applied to mitigate any vulnerabilities. IT department approval is necessary for software installations that may have access to sensitive data or systems.

Data Backup

All data must be classified according to its sensitivity level (e.g., public, internal, confidential). Access to sensitive data should be on a need-to-know basis, with appropriate user permissions assigned and approved by the IT department. Data backups should be performed regularly and stored securely by IT.

Password Policy:

Passwords must be unique, complex, and changed regularly (at least every 45 days) In case of suspected compromise, passwords should be changed immediately, and the incident should be reported to the IT department.

Network Security

All network devices must be configured securely with firewalls and intrusion detection/prevention systems. Wi-Fi networks should be encrypted and segregated based on access requirements. Remote access to the company network should only be granted through secure Virtual Private Networks (VPNs) with approval from the IT department.

Incident Reporting and Response

Employees must promptly report any IT security incidents to the IT department or designated authority, and the incident should be escalated to the immediate Manager or the Circle Head for

appropriate action. An incident response plan will be in place to handle and mitigate security breaches, with regular reporting to the C&R Head

Information Assets

- Equipment
- People
- Premises
- Third Parties
- Technology

Training & Awareness

Regular information security and cybersecurity training sessions will be conducted for employees to enhance their awareness of threats and best practices. New employees will receive information security and cybersecurity orientation during onboarding. Training and awareness is to change behaviours that have a large impact on the information security and cybersecurity.

Legal compliance

The Information Technology Act, 2000, is the primary legislation governing the use of technology in India.

Responsibilities

The head of the IT department is responsible for ensuring adequate control measures are in place after a risk assessment is conducted.

All staff are responsible for maintaining the information security policy and to protect all assets including hardware and software. Password management and patch management shall be duly complied with on a regular basis. Any incident that may cause a breach of this policy shall be reported immediately to their line manager and to the IT department.

The head of HR is responsible for ensuring timely information of new recruitments to the IT department and issuing IT assets during onboarding.

The head of IT department & Administrator are responsible for updating IT Assets & Finance is responsible to update monthly information to Managing Director

Head of IT department and head of C& R are responsible for Incident Response and its corrective actions. Records are part of this responsibility.

The IT department is responsible to ensure smooth functioning of this policy and sub policies and maintaining procedure and updating the same.

Revision Number	Date	Revised by	Approved by	Summary of changes
QAPA-P-05-Rev00	05 Aug 2023	Venkataram Arabolu	QACA Board	-