Capability BPO Group

Information Security Policy

Approved By:	Mark Essey
Effective Date:	25 May 2020
Review Date	1 December 2021
Document Owner	Group IT

Version Control

Record of changes applied and approved within this document.

Version	Date	Status	Drafted By	Details
1.0	04.07.2018	Approved	Mark Essey	Basic document outline
2.0	04.12.2018	Approved	Kevin Dry	Modernisation of Policy, involving complete re-write
2.1	13.11.2019	Approved	Kevin Dry	Revised for naming convention
3	14.05.2020	New Draft	Vivekni Haribhai	New version for authorisation
3.1	22.05.2020	Approved	Varesha Munsamy	Approved and finalised by ISO committee

Table of Contents

1. Introduction

1.1 Capability BPO Global (Pty) Ltd (**CBPO**), comprising of its affiliates, subsidiaries, and associated entities (collectively the **Group**) is committed to protecting and maintaining the Group's information assets from all types of threats.

1.2 The purpose of this Policy is to specify the requirements to be implemented within the Group to ensure that information systems within the Group are adequately protected and that appropriate measures are implemented for any deviations.

1.3 Accordingly, this Policy aims to develop, implement, continuously improve, mitigate against risks, and maintain a framework for compliance with the international best practices for Information Security.

2. Definitions

2.1 **Electronic communication** means any communication of information by electronic means;

2.2 **Electronic communications systems** mean all systems used by the Group that enable electronic communications, including (without limitation) the internet, electronic mail and any other means of digital media such as SMS and file transfers;

2.3 **Information Security** means the safeguarding of all information and information systems, including paper-based and physical environments, with due regard for the following primary security considerations:

- Confidentiality - ensuring that information is accessible only to those authorised to have access;
- Integrity - safeguarding the accuracy and completeness of information and its associated processing methods;
- Availability - ensuring that the authorised users have access to information and associated assets or systems, on a timely basis and when required.
- Identification and authentication - confirming the legitimacy of an individual or system, particularly in systems supporting electronic commerce;
- Non-repudiation - ensuring that the origination or receipt of information cannot be denied. This is particularly relevant when using systems supporting electronic commerce, as transactions cannot be repudiated and returned based on claims regarding the validity of its origination;

2.4 **Information system** means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes electronic communications systems;

2.5 **Policy** means this Information Security policy which is applicable to the Group;

2.6 **User** means a part- or fulltime employee of the Group, including but not limited to any contractor, consultant, business partners and / or any other third party with access to information of the Group;

3. Scope and Applicability

3.1 This Policy applies to the Group and all users within the Group.

3.2 To the extent that the Group have outsourced services with users, such agreements must be aligned with the provisions of this Policy.

3.3 This Policy forms the basis for implementing Information Security within Group and must be read in conjunction with all applicable laws, regulations, and supervisory requirements.

4. Objectives

4.1 Importance of Information Security

4.1.1 The Group acknowledges the importance of all information for the efficient operation of its business. Sound business decisions and operational competence necessitate that information is valid, accurate, complete, consistent, relevant, reliable, and available timeously.

4.1.2 The Group strives to build long term relationships with its customers and therefore is committed to utilising all information received in a manner which optimises its competitive advantage and efficiency in the local and global marketplace.

4.1.3 Therefore, it is essential that the Group's information and the supporting infrastructure are secured from threats such as manipulation or destruction, corruption, unauthorised access, processing of unauthorised or fraudulent transactions, unauthorised disclosure of client and other confidential information, or errors, whether inadvertent or intentional.

4.2 Privacy

The Group respects the privacy of all users granted access to its information resources and expects uses to use all information and digital media in a responsible manner. The Group therefore be entitled to monitor, intercept, and investigate any use wherein there is found to be abuse. As part of such investigation, it may be necessary to access and disclose private information and files of users.

4.3 Statement of Commitment

4.3.1 Information, in all forms, is a valuable asset to the Group. As such it is the responsibility of all users to protect, ensure the confidentiality of, integrity and availability of the Group's electronic and non-electronic information and/or systems, which includes but it not limited to information about employees, clients and products are valuable assets.

4.3.2 The Group's integrated approach to Information Security includes and involves all its business divisions.

4.4 Key Principles

4.4.1 Information Security of strategic and critical importance to the Group's business continuity and efficiency. Therefore, the following principles will direct deployment of resources for these purposes:

a) Practical and achievable implementation of safeguarding measures; and
b) Information Security will be an ongoing process and fully integrated with the overall processes to managing business risk within Group.

4.4.2 **The Information Security objectives are:**

a) Implementation of Information Security management structures and measures to effect and enforce compliance with the objectives, statements, policies, standards, and procedures.
b) Classification of information resources as to the level and type of protection required.
c) Proper identification and authentication of users.
d) The confidentiality of all data, information, systems, documents, and software will be ensured.
e) The integrity of data, information, systems, documents, and software will be ensured in accordance with its criticality.
f) Accountability and responsibility for user actions will be clear and enforced consistently.

g) Information and information systems should be available to authorised users in accordance with the business defined requirements. Resources will also be appropriately recoverable in the event of loss due to an undesired or unexpected event (e.g. system failure or natural disaster).
h) Appropriate physical and logical access control over information resources will be maintained in accordance with the classification of the specific resource.
i) All employees will be appropriately trained.
j) Clearly defined roles and responsibilities of all parties with access to information assets will be communicated.
k) All users must be familiar and comply with the Group's Information Security policies and procedures; and
l) Monitoring and reporting measures will be established to detect and report breaches of policy and to ensure remedial action.

5. Roles and Responsibilities

Information Security within the Group will be governed and supported by the existing business management structures. The specific roles and responsibilities in implementing and maintaining Information Security measures are:

ROLES	RESPONSIBILITIES
CEO	• Appointed as the information officer • Responsible to discharge all Information Security obligations • Entitled to delegate duties as deemed necessary
THE BOARD	• Ensuring that there is clear direction and visible management support for security initiatives • Approving Information Security Policies, Standards and Guidelines • Ensuring that exposures are periodically reviewed and assessed, as required
MANAGEMENT	• Ensuring alignment and synergy with Group IT and other business units' • Overseeing the implementation and ongoing monitoring of Information Security • Direct responsibility for ensuring that all users are aware of their Information Security obligations • Serve as security representatives for their respective business areas
GROUP IT	• Monitoring significant changes in the exposures of information assets to major threats • Keeping abreast with new developments in the information technology environment, and the security related impacts thereof
AUDIT	• Internal audits shall be conducted annually • External audits shall be conduct periodically, to the extent required

6. Group Information Security Policies

6.1 Data and Software classification, usage, and disposal

6.1.1 Classification

a) Owners must be assigned to all Group's data, information, and other information assets.
b) All data, information and other information assets will be classified as to its importance and sensitivity to the Group. For these purposes, an appropriate classification model will be applied.

c) Information assets will be safeguarded in accordance with such classification.
d) All cryptographic keys must be made available to Management.

6.1.2 **Usage**

a) The risks associated with information systems must be analysed using formal risk analysis methods and procedures. Security requirements and access rights must be defined in accordance with the associated business risks.
b) Access to information systems and data should be granted to authorised users only, to the extent required, to perform their day-to-day (or specific) functions.
c) Users are only entitled to access information, data, and information assets with the approval of the designated information owner.
d) Access rights must be reviewed regularly.
e) Users granted access to information systems must be clearly identifiable.
f) All information and data transfers must be done in a controlled manner with an adequate audit trail.
g) All information, digital media, data classified as confidential to the organisation, clients and business partners must only be disseminated with proper authorisation and adequately protected when transmitted over external networks.
h) Access to information shared via any form of networking must be properly controlled.
i) All programmes and documentation generated by or provided to users for the benefit of the Group remain the property of the Group.
j) The rights of employees and clients, with regards to the handling of their personal information, must be respected in accordance with statutory legislation.

6.1.3 **Disposal**

a) An information retention schedule should be compiled in accordance with the directives by management as well as legal and statutory requirements.
b) All information no longer required or useful must be deleted.
c) Sensitive electronic information must be deleted by means of overwrite functionality as the use of 'erase' will not suffice.
d) Prior to disposal, defective or damaged removable storage media containing sensitive information must be destroyed.
e) Sensitive information in hardcopy format should be disposed of by means of controlled shredding.

6.1.4 **Software**

a) A software register with the details of all software purchased or leased must be maintained. Access to the software register should be restricted to authorised personnel only.
b) No unlicensed software, shareware, public domain software or pirate software may be used on Group computer equipment unless explicitly authorised by a Group IT representative.
c) Users must comply with licensing or purchasing terms and conditions of suppliers.
d) All software should be disposed of appropriately. The disposal and associated actions must be authorised and details must be recorded in the software register.

6.2 Systems development and Change control

6.2.1 Applications, irrespective of whether acquired or designed and built, must comply with this Policy, standards, and procedures.
6.2.2 Information Security considerations must be addressed during development, implementation and change phases of the software life cycle.
6.2.3 All business applications and information technology infrastructure should be subject to documented change control procedures, including appropriate version control and back-out measures.

6.2.4 All software and/or hardware implementations within production business activities must be documented prior to its implementation.

6.3 Communication and network security

6.3.1 Virus protection

a) All computers must be protected by an approved virus protection package, which must be regularly updated.
b) Removable storage media should not be used until it has been checked for viruses.
c) Users must not attempt to eradicate viruses without expert assistance. If infection by a virus is suspected, users must immediately stop using the infected computer, disconnect from all networks, and contact the IT Department.
d) Users must not disable virus checking systems or attempt to introduce any malicious computer code designed to self-replicate, damage or compromise the performance of any of the Group's computer systems.
e) Users are prohibited from possessing any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept or monitor electronic communication (for example password cracking software, network sniffers etc.).

6.3.2 Logical access to network

a) Unauthorised access to telecommunication networks should be prevented by logical access controls. Unauthorised access attempts should be detected, reported and acted upon.
b) Logical access to the Group's network used by the Group should only be granted after proper approval.
c) All requirements for logical access and privileges should be reviewed on an annual basis.

6.3.3 Remote access connections

a) All users accessing the network remotely may only do so with prior consent and must comply with this Policy.
b) Remote access can be reviewed and terminated at any stage.

6.3.4 Internet and Intranet usage

a) Group Internet and Intranet connections are only to be used for valid business purposes and information exchange.
b) Internet and Intranet services should be used in accordance with the following:

standards of system etiquette.

- Users may not download files or software from the Internet unless authorised to do so by Group IT.
- Group standards of business conduct.
- any applicable national and international laws.
- Internet usage outside of business requirements is allowed only if it does not consume more than a trivial amount of resources; interfere with operational productivity; pre-empt any business activity; and / or portray the Group in any negative light.
- Group confidential information must not reside on either Internet or Intranet servers without proper security mechanisms being in place. Sensitive parameters (such as access codes, account details, credit card numbers or passwords) may not be transmitted unless authorised to do so. Intranets must either be shielded from external Internet users by firewalls or not be connected to external sources.

6.3.5 Networking

a) Access to and from untrusted networks is only allowed through a properly configured and authorised firewall infrastructure that filters traffic and prevents unauthorised access.
b) Modems connected to office desktop computers will only be allowed with explicit approval. Mobile and telecommuting microcomputers are the exception to this rule. Users needing to make connections with remote computers should only connect via the Group's standard modem infrastructure or via the Internet firewall.
c) If a dial-up connection is established from a workstation within the Group network to any other network, such as the Internet, the workstation must be disconnected from the Group network until the dial-up connection is concluded.
d) Users must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of the system support function.
e) The use of software that can remotely take control over a system must be properly controlled and only allowed if the owner of the target system authorises remote control.
f) Network configurations must be accurately documented.

6.3.6 E-Business security

a) Regular testing will be done against the IT infrastructure that supports e-business applications.
b) E-business applications will have an audit trail that will be reviewed frequently and acted upon as required.
c) E-business applications and the supporting infrastructure must be protected by means of perimeter defence mechanisms.
d) The Group will together jointly agree on standard way(s) to identify and authenticate clients.

6.4 User security

6.4.1 Passwords

a) Users must treat their identification mechanisms (e.g. passwords or PINs) in a responsible manner. Passwords should:

- Be a minimum of 8 characters in length.
- Comprise of at least one number and one special character.
- Not be easily guessable or words found in a dictionary.
- Not be shared or written down.
- Be changed regularly.

b) The use of a password not belonging to the user is not allowed.
c) Passwords must be kept confidential and not be provided and / or transmitted to any other user.
d) Users must not browse through the Group computer systems or networks, unless legitimately required to perform tasks.

6.4.2 Awareness and training

a) All users must be informed of the importance of Information Security.
b) Training in effective and secure computer usage will be available to all users as required.
c) Technical staff must be trained in the security disciplines required by the respective platforms.

6.4.3 Human resources practices

HR must take due cognisance of Information Security considerations.

6.4.4 **Workstations**

a) All Group workstations must be provided with a screensaver password, which must automatically activate after 15minutes.
b) When not in use, sensitive information and computer storage media should be securely stored and protected from unauthorised disclosure. Employees shall at all times endeavour to maintain a clean desk when same is unattended.
c) Users must not share their passwords with others.
d) On Group supplied computer hardware, users are not allowed to change operating system configurations, upgrade existing operating systems, or install new operating systems. Such changes shall require prior written approval from Group IT.
e) Computer and related equipment supplied by the Group must not be altered or added to in any way.

6.4.5 **Business Use only**

a) Group information (inclusive of Group stationary such as company logo, letterheads etc.) resources should be used for business activities only.
b) Users are not permitted to use Group information resources for charitable endeavours or private business activities.

6.5 Asset Accountability

6.5.1 An asset register shall be maintained and updated periodically.
6.5.2 All portable equipment of whatever nature should not be moved or relocated without approval of the relevant manager and there shall be no tampering of asset tags.

6.6 Business continuity

6.6.1 All sensitive, valuable, or critical information resident on Group computer systems must at least monthly be backed-up.
6.6.2 Plans and arrangements are to be implemented to enable the continuity of business-critical functionality under conditions of disruption to normal operations such as:

a) formulating controls to identify and reduce risks to an acceptable level;
b) ensuring quick, effective, and orderly response to incidents; and
c) timely resumption of essential operations and the limitation of consequences of damaging incidents.

6.6.3 Disaster recovery and business continuity plans are to be regularly tested by the Group IT.

6.7 Monitoring and Compliance

6.7.1 **Exceptions to the Group Information Security Policy**

a) The Group acknowledges that there may be circumstances in which non-compliance with this Policy may be required. Non-compliance must be authorised by means of a risk acceptance process, which requires a risk acceptance memorandum to be signed by a manager and approved by the Board in writing prior to such non-compliance taking place.
b) If policy exceptions will circumvent existing internal controls, then mitigating controls must be implemented and followed.

6.7.2 **Violation**

a) All users of information will be held accountable for their use of information resources.
b) Non-compliance or violation of this Policy will result in actions that may include the following:

- Restricted access to electronic information and / or possible suspension of employment;

- Other disciplinary action which may lead to termination of employment; and/or
- Civil proceedings and/or criminal prosecution.

c) Sanctions against contract employees will be in accordance with the terms of their contract.

6.7.3 **Incident management and notification**

A formal process must be maintained to investigate and regularly report on Information Security incidents and the resolution thereof. Users must promptly report all information security breaches, warnings, and the like to Management and must not forward such information to other users.

6.8 **Electronic contracting**

6.8.1 Users, without authorisation, shall not make statements that bind the Group in any manner.
6.8.2 Users may not make use of scanned versions of hand-rendered signatures to give the impression that any electronic communication has been signed.

6.9 **Encryption of electronic communications and devices**

6.9.1 Employees should note that most electronic communications are by default not secure.
6.9.2 Electronic communications may only be encrypted utilising technologies approved.
6.9.3 All company owned external hard drives are to be encrypted by means of Bitlocker.

6.10 **Acceptable and unacceptable use**

Electronic communication systems shall not be used for:

6.10.1 receiving or transmitting any discriminatory, obscene, offensive, profanity, obscenities, derogatory remarks discussing employees, customers, competitors or others;
6.10.2 any defamatory, discriminatory, or obscene material;
6.10.3 infringing on another person's (whether natural or legal) intellectual property rights (e.g. copyright);
6.10.4 carrying messages which may be seen to be insulting, disruptive, offensive to other employees or could lead to a breach of confidentiality;
6.10.5 any attempt to penetrate or to gain unauthorised access (or attempted access) to the electronic communication systems or network security of the Group or other third party system;
6.10.6 the violation or attempted violation of any law; or
6.10.7 disclose any secret or confidential information, whether requested via an internal or external source, without approval of the Board.

6.11 **Electronic communications notice**

The standard disclaimer is to be included in all electronic communication, which disclaimer shall be subject to review and amendment from time to time.

6.12 **Policy maintenance**

a) This Policy is subject to amendment by the Board and / or the legal representative of the Group.
b) Version control will be applied, which will include the version number and date. After each amendment thereto, the latest version will be distributed to all relevant parties.
c) It is the responsibility of all information asset users to ensure that they are kept up to date with the changes.