PRIVACY & INFORMATION SECURITY POLICY

Purpose:

The purpose of the Policy is to establish and maintain the confidentiality, integrity and availability of information, information systems, applications and networks owned or held by FORTCAPS

- Confidentiality:
  access to data should be confined to those with appropriate levels of authority - unauthorised access should be prevented;
- Integrity:
  safeguard the accuracy and completeness of data- prevent unauthorised accidental or deliberate alteration;
- Availability:
  Data should be available and delivered to the authorised individual in a timely manner – prevent non availability of systems

Applicability:

This Policy is applicable to any person (management, employees, contractors and third parties) who access information or assets of the company whether they access the system from the company's office(s) or remotely.

Coverage of information assets:

The Policy and standards contained in this document have been established to cover information / data, software, hardware, networks and information processing facilities used by the company.

More specifically, the Policy applies to, but not limited to, the following information assets of the company:

- All proprietary information that belongs to the company
- Personal information relating to employees of the company
- Personal information relating to customers held by the company
- Personal information relating to supplier, contractor and other third parties held by the company
- All hard copies document held by the company
- All software assets such as application software, system software, development tools and utilities of the company
- Websites, portals and other information systems of the company
- All physical assets, such as computer equipment, network and communications equipment, media and equipment relating to facilities of the company
- All services, such as power, lighting, HVAC ((heating, ventilation and air-conditioning) associated with the company's information systems

Managements Roles and responsibilities

- support implementation of Information Security controls within their areas of operations

- ensure that employees, contractors and third parties under their control, who access information or assets of the company are aware of, and adhere to, this Policy and the standards

Employees Roles and responsibilities

- be aware of and comply with the security requirements that are currently in force
- be individually responsible for the security of their physical environments (conference rooms, desk, common work area, etc.)
- ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard regardless of where it resides
- abide by organisational and relevant legal and regulatory requirements
- report any suspicious and/or non-compliant behaviour or system vulnerability in information security controls

Enforcement:

Compliance with the Information Security Policy is important to the company. Failure to comply with this Policy may result in disciplinary action, and the imposition of a disciplinary sanction (up to and including the immediate termination of employment), as well as criminal and / or civil action.

It is a condition of employment that those employees who obtain and / or process personal data adhere to the rules of this Policy.

The company may at any time update this Policy to comply with changes in the legislation and / or its internal organisation and procedures. The updated version of the Policy will be communicated to the relevant persons.

Policy rules:

Asset inventory and acceptable IT usage

To achieve and maintain appropriate protection of organisational assets and information. This Policy is intended to identify critical assets and their owners and to ensure that critical IT assets are used for legitimate purposes only.

- An inventory and ownership of all important assets should be drawn up and maintained.
- Acceptable use of information and information assets should be followed by all employees, and relevant contractors and third parties.

Human Resource and Information Security

To ensure that employees, contractors and third party users

- understand their responsibilities, and are suitable for the roles they are considered for
- are aware of information security threats and concerns, their responsibilities and liabilities.

- Joining process-
  To reduce the risk of theft, fraud, misuse or human errors, reference checks / background verification checks should be carried out for the new joinee to the extent the local laws permit.
  The reference checks may cover one or more of the following, subject to local regulatory or legal restrictions.
  - Identity of the person
  - Education
  - Work history
  - References

  The company expects that information disclosed to its employees will be treated with the appropriate level of confidentiality; therefore the employees are under an obligation to maintain the confidentiality and secrecy of the sensitive information accessed by them in the course of their employment.

- Security awareness:
  Respective managers should ensure that employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities and are equipped to support information security in the course of their normal work.

  In order to achieve this,
  - Information security awareness and awareness of this Policy should be included as part of induction training for new joiners.
  - Changes to the Policy and other related policies and standards should be communicated to all employees and relevant contractors and third parties.
  - Information Security awareness communications should be sent to employees periodically.

- Separation process:
  Upon termination of their employment,
  - all employees, contractors and third parties should return all of the organisation's assets in their possession
  - the employee's physical access privileges to the facility and logical access to applications and infrastructure should be revoked through the exit process immediately on leaving.

Third party Services

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

In order to achieve this,

- agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities must cover all relevant security requirements.
- clauses on confidentiality, non disclosure and protection of personal data are included in the contract agreements with third parties.
- physical and logical access to the company's computer systems is restricted to third party contractors on a "Need to Know" basis.
- Outsourced software development is supervised and monitored.

Privacy

- Protection of Privacy Data should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
- Identifying and protecting the personal information of foremost importance.
- Personal data should be collected, used, processed, retained or disclosed only for the purpose identified.
- Personal data should be retained for a period as specified by respective laws and respective entity's retention policies. Personal data is deleted / erased securely after completion of retention period as specified in the retention policies.
- Access to personal information should be provided to employees / third party service providers based on the company's Privacy Policy and only on need to know basis.

Physical access and environmental controls

To prevent unauthorised physical access, theft, damage, interference to the organisation's premises and information.

To protect the information assets from security threats and environmental hazards that may cause interruptions to the organisational business activities.

Availability of information assets for business activities may be greatly impacted when physical security is compromised or the information assets are affected by threats such as power failure, flood, fire or technical error.

In order to protect information assets against physical or environmental threats, the following security measures should be taken:

- Physical protection to Buildings
  The access to the factory office buildings must be sufficiently controlled. Visitors should only have restricted access to the company's premises.

- Physical protection to Data Centres / Server rooms
  - Critical infrastructure components like servers, network switches and storage components must only be placed in data centres / server rooms.
  - Physical access to the data centres / server rooms should be controlled through electronic access card system or biometric devices or a combination and it must be ensured that the access is restricted only to authorised persons.
  - Physical access to data centre / server rooms should be granted only after approval by IT Manager / responsible authority.
  - Access to visitors to the data centre / server rooms should be restricted and monitored.
  - Access requests by visitors to the data centre / server room should be approved by an authorized person and visitors should be escorted by authorized persons.
  - Visitors should sign a visitors' log, record entry and exit time and purpose of visit.
  - Data centre/ server room visitors' log should be reviewed on a monthly basis to verify the appropriateness of visits.
  - Video monitoring and intruder detection may be in place, where required and feasible, subject to legal and regulatory restrictions on video surveillance.
- Environmental Protection
  - Smoke detectors, fire alarms, fire suppression systems, air conditioners, UPS and Power backup generators should be installed to protect the information assets from environmental threats.
  - These equipment should be tested and maintained on periodic basis to ensure the environmental protection systems provide continuous support.
  - Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Logical access controls

The following logical access controls should be implemented for accessing Network, Domain, System software, Database and Applications.

- Prior approval from an authorised person is required to create or modify user accounts and access rights of employees, contractors and third parties. The user access request should specify for whom the request is required and what accounts and access rights are requested and approved.
- Logical access to users should be provided based on their roles and responsibilities in the organisation. Access should be granted based

on the principles "segregation of duty (SOD)", "least privileges" and "need to know basis".

- Administrator or privileged user access should be restricted. All users should have separate user id for their personal use only. Users should not share their passwords.
- Administrator or other user accounts should not be shared.
- User accounts and access rights of employees, contractors, third parties should be deleted or disabled or removed immediately upon termination.
- A half yearly review of user accounts and access rights should be performed by the respective managers to identify and delete / disable inappropriate accounts or access rights.
- Vendor provided default user accounts should be deleted or disabled or renamed unless required for the system operations. If these are required for system operations, default passwords should be changed for such accounts.

Authentication - Password security

Intruders, hackers or any unauthorised persons may exploit an information system with no password or a weak password security to gain unauthorised access and cause severe damage to the information contained within the system. This may lead to direct and indirect losses such as financial, reputational, legal, compliance losses.

- Recommended password control standards should be applied to all information systems within the company.
- Logical access to information systems should be permitted only after an identification and authentication process.
- For default / vendor provided user accounts that are necessary for the operations, default password should not be used. Default password should be changed at the time of installation.
- Users should not enable "Remember Password" option for any internal / web based logins.

Network and system security

Networks and systems must be adequately managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

- Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
- Firewalls should be placed in the network to prevent unauthorised access to the network. Firewall logs should be enabled and stored for a specified future period.
- Latest service packs and patches should be applied as appropriate

- Vulnerability assessments should be conducted periodically

Antivirus deployment and usage

To prevent and detect the introduction of viruses and other malicious codes and to ensure that preventive, detective and corrective measures are in place to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).

Following controls should be implemented to protect the network and computer system from malwares:

- Endpoint protection/antivirus software should be installed on relevant infrastructure.
- Endpoint protection/antivirus server should be configured to download recent definitions from the vendor website automatically.
- Other servers, client computers, desktops and laptops should be installed with the client version of the endpoint protection / antivirus software.
- It should be configured to ensure that the client version of the endpoint protection / antivirus software is automatically updated on a daily basis or more frequently.
- "Auto protect" feature and periodical scanning should be activated.
- End users should not be provided with administrative access to change the configuration settings or stop running the antivirus services in their desktops or laptops.
- Users should not open suspicious mail attachments or unknown file types.
- In the event of any system is infected by virus, it should be immediately reported to the IT responsible authority. Only the authorised IT employee should handle the incident

Change management

- When significant infrastructure or application changes are proposed / implemented, the impact on information security, data privacy and controls should be evaluated and issues, if any, should be addressed appropriately. If required, Information Security Policy and list of controls are updated and communicated to relevant employees and third parties.
- When new applications are developed or changes are made to existing applications, necessary input and output validations should be identified and implemented to ensure accuracy of information.
- Infrastructure and application changes should be logged, documented and tracked through to completion.

- Development and Test environments should be physically or logically separated from the production environment.
- Relevant tests (such as capacity and performance test, security configuration test, interface test, integration testing, regression testing and Functionality testing) as applicable should be conducted for significant infrastructure and application changes and the test results should be reviewed prior to implementation.
- Infrastructure and application changes should be assessed and approved prior to implementation in production. In case of emergency changes, depending on the situation, the approval may be obtained after implementing the change.
- Ability to make changes to the production environment should be restricted to authorised personnel.
- Access to program source code should be restricted.

Information backup, restoration and media handling

Data backup is vital for the business as it is the key component in ensuring Business continuity in case of loss of primary data or non availability of information systems associated with primary data.

- Data should be backed up on a regular basis
- The type of backup and frequency should be decided based on the business requirements.
- The Backup procedures and backup data retention requirements should be documented and followed (backup frequency, type of backup, full backup, incremental or differential backup, what data is backed up and media rotation etc.)
- Backup data retention period should be in line with the data retention for the primary data. Backup media should be periodically tested for restoration of data.
- Access to backup data and backup media should be restricted to authorised individuals. Backup media should be securely stored or transported.
- Backup of the video images should also subject to the same retention policy and security requirements.
- Media should be disposed off securely using procedures such as degaussing, shredding so that the information contained in the media cannot be recovered or reconstructed.

Incident and problem management

- All must promptly identify, report and respond to any incident or suspicious activity observed or suspected, which affects or may affect security, through appropriate management structure.

- Incidents and / or problems including security incidents should be logged, prioritized and assigned to appropriate team / persons and timely escalated and tracked to resolution.

Email security

To ensure that email services are utilised in ethical and lawful manner for business purposes only. The risks that are inherent to email communications are identified and addressed appropriately to protect the organisational information from security threats.

- Monitoring:
  To the extent permitted by law, the company will monitor and access any and all aspects of email and Internet use for business purposes; users must not assume that any information created using the company email and Internet or any communication transmitted over the company systems are or will be private; Email and Internet may be subject to company back-up and archive procedures and subject to review by legal staff and third parties in connection with legal proceedings. Employees must co-operate by providing access to Internet or other email communications made through the company's resources, if required, for support, investigation or other business needs.
- Controls that should be implemented for preventing spread of virus, worms and other malware through email servers:
  - Incoming and Outgoing email traffic must be scanned for viruses, spam and other malware.
  - Incoming spam should be centrally quarantined with the possibility for the employee to access his / her quarantined email.
  - Virus and anti-spam definitions on the email servers and gateways should be updated as soon as possible after they are released by the vendor.
  - Automatic forwarding of the company emails to non-company mailboxes must be disallowed.
  - Administrative access to mail server should be restricted to limited authorised users

CCTV usage

To monitor the visitors to the facility at permissible points to deter, prevent, detect and analyse physical access intrusion.
To define the controls required to be adhered while using CCTV operations in order to protect the privacy of the visitors and to meet the regulatory and legal requirements

- The system must be used as a proportional response to identified problems and used in the interest of safety at the work place, detection of security breaches and loss prevention.

- All applicable legal requirements must be met in planning the camera installation; the operational procedures must ensure that evidence is secured, retained and made available to ensure the absolute respect of the right to privacy.
- Monitoring and recording (the equipment must be operated by trained and authorised users only, non-disclosure agreements must be signed by the identified personnel engaged in operating and managing the CCTV equipment);
- Retention of recorded information (data must be retained as foreseen by applicable laws; back-up copies may be maintained if required; data pertaining to any security incidents must be retained until closure of the case as required or as dictated by applicable laws).
- Cameras should only be installed at main entrances and exits of the workplaces and buildings and certain other strategic locations.
- Signs should be displayed to indicate that surveillance cameras are being used.
- The video images should be used only for surveillance purposes unless the footage is needed for an investigation.
- Surveillance video images are erased securely after the prescribed period unless the footage is needed for an investigation.
- Physical and logical access controls should be implemented for the computer system and media containing surveillance video images. Access rights are limited to a small number of clearly identified individuals on a strictly need-to-know basis.
- Only the "controller", the system administrator, or other staff member/s specifically appointed by the controller for this purpose can grant, alter or remove access rights of any persons.
- Backup of the video images are also subjected to the same retention policy and security requirements
- Once the video footage recorded media is no longer useable (after many cycles of use) it should be safely disposed off in such a manner that the remaining data on it would be permanently and irreversibly deleted
- The personnel monitoring the surveillance camera footage should not have access to the recorded data. The footage cannot be copied into removable media unless required for evidence purpose during inquiry or investigation.
- No generic or common usernames and passwords are allocated to employees of an outsourced security organisation.

REPORTING GRIEVANCES

Data Privacy Officer,
Fortcaps Healthcare Ltd
Plot 86-92 Sector I
Govindpura Industrial Area
Bhopal MP 462023
Email dpo@fortcaps.com