DICABS®

DIAMAOND POWER INFRASTURCTURE LTD

Corporate Office: A2- 12th Floor, “Palladium”,
Near Orchid Wood, Opp. Divya Bhaskar,
Corporate Road, Makarba,
Ahmedabad 380 051 Gujarat
CIN No.: L31300GJ1992PLC018198
Website: www.dicabs.com

Information Security ISMS Policy

(Effective from 10.11.2025)

TABLE OF CONTENTS

1.0 PURPOSE

To ensure that appropriate security measures are adopted to protect against Information Security risks.

2.0 SCOPE

Entire Information Security of ISMS Security of the company.

3.0 DEFINITION

DICABS: Diamond Power Infrastructure

4.0 RESPONSIBILITY

IT-Head/Third Party Service Provider/Maintenance Head is overall responsible for ensuring that the policy is followed.

5.0 SECURITY POLICY

5.1 Introduction

The Information Security Policy provides an integrated set of protection measures that must be uniformly applied across Diamond Power Infrastructure (DICABS) to ensure a secure operating environment for its business operations.

Customer Information, organizational information, supporting IT systems, processes and people that are generating, storing, and retrieving information are important assets of DICABS. The availability, integrity and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance, and respected company image.

This Information Security Policy addresses the information security requirements of:

- **Confidentiality:** Protecting sensitive information from disclosure to unauthorized individuals or systems.
- **Integrity:** Safeguarding the accuracy, completeness, and timeliness of information.
- **Availability:** Ensuring that information and vital services are accessible to authorized users when required.

Other principles and security requirements such as Authenticity, Non-repudiation, Identification, Authorization, Accountability, and audit ability are also addressed in this policy.

5.2 Scope

- This policy applies to all employees, contractors, partners, Interns/Trainees working in DICABS. Third party service providers providing hosting services or wherein data is held outside DICABS premises, shall also comply with this policy.
- Scope of this Information security Policy is the Information stored, communicated, and processed within DICABS and DICABS's data across outsourced locations.

5.3 Objectives

The objective of the Information Security Policy is to provide DICABS, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services.

5.4 Periodic Review

The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures, by DICABS Management.

This policy will remain in force until next review / revision.

5.5 Policy Compliance Check

Compliance review of IS policy should be carried out by Internal/External auditor on a periodic basis. Inspection & Audit Division is responsible for monitoring compliance of IS Policy.

5.6 Information Security Governance

Information security governance consists of leadership, organizational structures and processes that protect information and mitigation of growing information security threats.

Critical outcomes of information security governance include:

- Alignment of information security with business strategy to support organizational objectives.
- Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.
- Management of performance of information security by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved.
- Optimization of information security investments in support of organizational Objectives.

It is important to consider the organizational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

5.7 Policies, Procedures and Guidelines

At DICABS considering the security requirements, Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below.

6.0 ASSET MANAGEMENT POLICY

Information assets shall be accounted for and have a nominated asset owner. Owners shall be identified and catalogued for all information assets and the responsibility for maintenance of appropriated controls shall be assigned. The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains accountable for the proper protection of the assets.

- All IT assets purchased by the DICABS are the property of DICABS and will be deployed and utilized in a way that is deemed most effective for addressing the DICABS needs and objectively demonstrates value for money.
- For compatibility and efficiency reasons, IT assets will be issued on a 'fit for purpose' basis based on predefined user roles using standard equipment as detailed on the approved hardware and software lists.
- Enquiries about and requests for individual IT assets must be submitted to the IT Head via the IT Service Desk in accordance with current ordering processes and procedures.
- All IT assets must be assigned to individual users or to a department who will always be held responsible for their care and security whether they are in use, storage or movement.
- Information about all IT assets will be held in the asset management system, which will be maintained by the IT Team, to enable them to be tracked, managed and audited throughout their entire lifecycle.
- IT assets will be adequately administered and maintained to ensure they remain fit for purpose and compliant with the licensed conditions of use during their entire lifecycle.
- Individual users or departments will be held responsible for protecting the IT assets that have been assigned to them against physical or financial loss whether by theft, mishandling or accidental damage by using appropriate physical security measures.
- End users are not allowed to install unapproved software on devices. Requests should be made to the IT Service Desk to have additional software that is not on the approved hardware and software list installed on to a device. Any software installed must be legitimately purchased and licensed for the use made of it.
- End users must always contact the IT Service Desk if they need to move, reassign or return IT equipment.
- All IT assets that are no longer in use must be returned to the IT Dept. via the IT Service Desk for redeployment.
- In order to ensure the confidentiality of information, any IT asset that has been used to process or store personal or sensitive information will be wiped before being reissued and must go through a physical disposal and destruction process at the end of its useful life as defined.
- The management of IT assets must comply with this policy. Breach of this policy may result in any device being remotely wiped, blocked from the DICABS's network and being prevented from using DICABS provided services and software. A breach may also be considered a disciplinary offence.

7.0 INFORMATION RISK MANAGEMENT PROCEDURE

Detailed risk assessments for Information risks (e.g. application risk assessment, Infra risk assessment) shall be undertaken in order to identify pertinent threats, the extent of vulnerability to those threats, the likelihood and the potential impact should a threat mature as a result of the vulnerability. This assessment shall determine acceptable, transferable, and avoidable risk and the risk that shall be reduced by risk treatments (control mechanisms).

- A thorough analysis of all **DICABS** information networks and systems will be conducted on a periodic basis to document the threats to and vulnerabilities of stored and transmitted information. The analysis will examine the types of threats -- internal or external, natural, or manmade, electronic, and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination, and protection.

  From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

- Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

8.0 ACCESS CONTROL POLICY

Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized. The Access Control Policy addresses this need.

- **Authorization:** Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

  i. **Context-based access:** Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.
  ii. **Role-based access:** An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
  iii. **User-based access:** A security mechanism used to grant users of a system access based upon the identity of the user.

- **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

i. At least one of the following authentication methods must be implemented: 1. strictly controlled passwords, 2. biometric identification, and/or 3. tokens in conjunction with a PIN.
ii. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.
iii. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).
iv. The user must log off or secure the system when leaving it.

9.0 E-MAIL SECURITY POLICY

DICABS shall implement effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication and implement control procedures so that the e-mail facility is not misused by the users. It also needs to be ensured that e-mail service and operations remain secure, efficient while communicating within intranet as well as through the internet.

- All use of email must be consistent with DICABS policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- DICABS email account should be used primarily for DICABS business-related purposes; personal communication is permitted on a limited basis, but non-DICABS related commercial uses are prohibited.
- All DICABS data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a DICABS business record. Email is a DICABS business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a DICABS business record shall be retained according to Record Retention Schedule.
- The DICABS email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DICABS employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding DICABS email to a third-party email system. Individual messages which are forwarded by the user must not contain DICABS confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct DICABS business, to create or memorialize any binding transactions, or to store or retain email on behalf of DICABS. Such communications and transactions should be conducted through proper channels using DICABS-approved documentation.

10.0 INTERNET & INTRANET SECURITY POLICY

DICABS should utilize Internet as an important resource for information and knowledge to carry on the business more efficiently. Users must also understand that any connection to the Internet offers an opportunity for unauthorized users to view or access corporate information. Towards this direction, DICABS has developed systems & procedures to ensure that Internet is used only for business purposes in a secure manner (without endangering the security of DICABS's network) with a uniform code of conduct.

- DICABS's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of India.
- Use of DICABS's resources for illegal activity is also deemed a disciplinary offence and will be dealt with under DICABS's procedure, and the DICABS will cooperate with any legitimate law enforcement activity.
- Any software or files downloaded via the Internet onto the DICABS network or local hard drive become property of DICABS.
- Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
- Large files, such as .mpg files, "music on demand" or any other "entertainment media" files should not be downloaded.
- Media streaming is forbidden due to the negative impact it creates on the performance of the network. Should this access be a work-related requirement, formal approval should be sought from the IT Support team.
- No employee may use DICABS facilities knowingly to download or distribute pirated software or data.
- No employee may use DICABS's Internet facilities to propagate deliberately any malicious code (e.g. virus, worm, Trojan Horse or trap-door program) that is designed to interfere with the normal running of other users' machines or applications.
- No employee may use DICABS's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Each member of staff using DICABS's Internet facilities shall identify himself or herself honestly, accurately and completely when participating in online discussion groups or similar, or when setting up accounts on outside computer systems.
- Only those employees who are duly authorized to speak to the media, or to analysts or in public meetings on behalf of DICABS may speak/write in the name of the Trust on online discussion forums.
- Where an individual participant is identified as an employee or agent of DICABS, he/she must refrain from any unauthorized political advocacy or from the unauthorized endorsement or appearance of endorsement by the organization of any (commercial) product or service not sold or provided by the DICABS, its subsidiaries or its affiliates.
- Employees are reminded that online discussion forums are public areas where it is inappropriate to reveal confidential DICABS information of any sort, including patient or employee data, professional secrets, financial data or any other material covered by

existing DICABS policies and procedures on confidentiality, or any other material that could identify these subject matters.

- Staff must not under any circumstances use the Internet to conduct personal commercial or business activities.

11.0 PASSWORD SECURITY POLICY

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change All Application software in DICABS will have to comply with minimum password standards as specified in this document.

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Users are responsible for complying with the following password standards:

- Passwords must never be shared with another person unless the person is a designated security manager.
- Every password must, where possible, be changed regularly -- (between 45 and 90 days depending on the sensitivity of the information being accessed).
- Passwords must, where possible, have a minimum length of eight characters.
- Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
- Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
- When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc....). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:

- Passwords routed over a network must be encrypted.
- Passwords must be entered in a non-display field.
- System software must enforce the changing of passwords and the minimum length.
- System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15-minute timeframe. Lockout time must be set at a minimum of 30 minutes.
- System software must maintain a history of previous passwords and prevent their reuse.

12.0 OPERATING SYSTEM SECURITY POLICY

DICABS shall protect its operating system resources by providing security at a level that is appropriate for the nature of the data being processed. The operating system security policy has been framed for achieving this. DICABS shall protect all business data, related application systems and operating systems software from unauthorized or illegal access. Access to the operating system must be restricted to those people who need access to perform their duties.

13.0 NETWORK SECURITY POLICY

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorized access. DICABS's Network infrastructure needs to be protected from unauthorized access. A range of security controls is required in computer networks to protect these environments.

13.1 Risk Assessment

The Information Security Manager, working in conjunction with the Network Manager, will be responsible for risk assessing, and reporting upon, the Trust's network.

- Risk assessments will be conducted on the network annually, the scope of the risk assessment will change depending on which area of the network requires assessing.
- Risk assessments will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the Network.
- Formal risk assessments will be conducted using CRAMM methodologies and will conform to ISO27001 standards.
- Regular vulnerability assessments / penetration tests will be performed to ensure compliance with defined controls.

13.2 Physical and Environmental Security

- Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive Network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality
- All public network facing firewalls will be accredited to Common Criteria EAL4 / Protection Profile compliant as a minimum.
- All unused network ports will be unpatched to minimize the likelihood of unauthorized equipment being connected to the network.
- Areas which are controlled with secure key-code locks will be periodically changed, following a compromise of code or when a member of staff leaves.
- Critical or sensitive Network equipment will be protected from power supply failures.
- Critical or sensitive Network equipment will be protected by intruder alarms and/or CCTV and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive Network equipment.
- All visitors to secure Network areas must be authorized by a senior member of the IT department.
- All visitors to secure Network areas must be made aware of Network security requirements.
- All visitors to secure Network areas must be logged in and out. The log will contain name, organization, purpose of visit, date, and time in and out.
- The Information Security Manager will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted when necessary.

13.3 Access Controls

Access to Secure Network Areas -- DICABS Staff

- Access to secure network areas is restricted to only those staff who need access to the area as part of their role.
- Access to secure areas are regularly reviewed and ensure that the list is accurate and up to date.

Logical Access to Network -- All DICABS Staff

- All access to the network must be via a secure log-on procedure, designed to minimize the opportunity for unauthorized access.
- Ensure a formal registration and de-registration procedure to access the network, with line manager authorization.
- Access rights to the network must be allocated based on the user's job rather than user's status within the organization.
- User access rights (as configured in Active Directory) will be removed or reviewed when a user leaves the organization or changes job upon notification from the HR department.
- Security privileges must be granted to those that require access. This access is limited to trust Staff whose role requires them to have System Administrative access.
- All users must have an individual user identification (username) and password.
- Users are responsible for ensuring that their username and password are kept safe.
- Generic/shared user identification and password will only be granted with a justifiable business requirement and must be only used for the purpose they have been created for. Approval can be sought from the Information Security Manager.

Third Party Access to the Network

- Third party access to the network will be based on a formal contract that satisfies all necessary NHS, and Data Security & Protection Toolkit security conditions.
- All third-party access to the network will be managed and logged on the DICABS's service-desk system.

Connections to External Networks

- All connections to external networks and systems conform to the Network Security policy, Code of Connection, the Electronic Communications policy and supporting guidance.

Access via VPN (Virtual Private Network) -- All DICABS Staff

- The VPN token will only be issued after the completion of the user acceptance form. Completed forms are held by the IT department.
- Access will only be provided to DICABS managed devices.
- All users must conform to the Acceptable Use policy (as if connected to the local network).

14.0 ANTI-VIRUS POLICY

Virus, Trojans, Worms, etc., are malicious programs called malware and can corrupt or destroy data or may spread confidential information to unauthorized recipients, resulting in loss of Confidentiality, Integrity, availability of the information. Malware detection and prevention measures as appropriate need to be implemented. The basis of protection against Malware should be founded on good security awareness and appropriate system access controls.

Users must keep approved and current virus-screening software enabled on their computers. This software must be used to scan all software coming from third parties or other DICABS departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for damage occurring because of viruses on computer systems under their control. As soon as a virus is detected, the involved user must immediately call the Information Technology department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

All personal computer software should be copied prior to its initial usage, and such copies must be stored in a safe place. These master copies can be used for recovery from computer virus infections, hard disk crashes, and other computer problems.

DICABS computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a testing regime approved by the IT Head.

14.1 Deployment of Antivirus:

- For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed.
- In a networked environment, an antivirus server should be deployed, and all the workstations should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as updating of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally with the antivirus server in order to have a centralized monitoring of all the activities.
- Identify all the possible entry points in the network through which a virus attack is possible and all the traffic entering the network through these points should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the

network, whether be it HTTP, FTP, SMTP or POP3. This ensures that the risk of any virus entering the network by any means is greatly reduced.

- Application based Antivirus should be installed for applications like MS-Exchange, Lotus Notes etc.

14.2 Integration of Antivirus with Other Tools

Content Filtering:

Mobile Malicious Code like unsigned ActiveX, MIME, java applets are routes of possible virus infection. Content Filtering should be used for protocols like HTTP/SMTP/POP3/FTP. Antivirus Software is to be integrated with Content Filtering Software.

Firewall:
A firewall with Antivirus support will give additional security for the network.

14.3 Best Practices:

- A good anti-virus i.e. Quick Heal Enterprise Edition product should be chosen for DICABS. A centralized server-based antivirus i.e. Quick Heal Antivirus system is deployed at DICABS with a computer network.
- The latest version of the antivirus with the latest signature is required to be loaded in all the machines of the organization. This is important as new and more potent viruses are discovered every day and even a few month-olds anti-virus program may be ineffective against newer viruses.
- For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
- For a networked environment there must be a central server to check for viruses' in all the machines automatically.

The following schedule is used for a full scan of the PC's.

a.Servers:Daily
b. Workstations:

- Daily Schedule the operation when there is least human interaction with the workstations.
- The antivirus software should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.
- External media (ex. Floppy, CD's) is one of the most potent medium for transmission of viruses', hence it must not be used in the network except for a few pre-determined PC's.
- Anti-virus logs should be maintained for a period of 7-15 days in the organization.

- The mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block or remove email that contains attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.
- To prevent spamming to mails in the DICABS, mails only authenticated by users in DICABS should be allowed.
- All employees must be made aware of the potential threat of viruses and the various mechanisms through which they propagate.
- Employees must be trained not to open attachments unless they are expecting them.
- Do not allow user to execute software downloaded from internet unless certified safe by system administrator.
- Always keep patch level up-to-date, especially on computers that host public services and are accessible through the firewall. Such as HTTP, FTP, mail and DNS services.
- In the case of a virus attack the following steps are required to be taken.
    i. The network share of the machine has to be stopped.
    ii. The contact person for cleaning the machine of virus has to be notified.
    iii. A mechanism is in place where an authorized expert/workstation is notified automatically in case of a virus attack.
- The notified expert should perform the following action on the infected workstation.
    i. Determine the type of virus.
    ii. Isolate all infected systems and floppy disks.
    iii. Try to clean the infected file.
    iv. In case of failure above the file should be deleted from the workstation.
    v. In case of failure above the workstation should be removed from the network and remedial action taken.
    vi. Remedial action may include reformatting depending on the severity of the problem and as per specific policy of the company.

15.0 BACKUP & RECOVERY POLICY

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures have been developed for backup of all business data, related application systems and operating systems software on a scheduled basis and in a standardized manner across DICABS. The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly.

Personal computer users are responsible for backing up the information stored on their local machines. For multi-user computer (servers) and communication systems, a system administrator is responsible for making periodic backups.

To ensure that valuable or critical data is backed up, it must be stored on network servers managed by the Information Technology department or a trusted partner.

DICABS requires the use of industry-standard media, techniques, and timelines in executing all backups. For multi-user computer systems, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and during the off hours.

Storage of backup media is the responsibility of the office computer user or multi-user computer system administrator involved in the backup process. Media should be stored in fireproof safes, at a separate location at least several city blocks away from the system being backed up.

Information listed on the Information Retention Schedule maintained by the Business Office, must be retained for the period specified. Other information must be properly disposed of when no longer needed, which is generally within two years.

Department managers are responsible for preparing, testing and periodically updating department contingency plans to restore service for all non-IT managed production applications and systems. The Information Technology department is responsible for preparing, testing and periodically updating network service contingency plans. All Confidential information stored on backup media should be encrypted using approved encrypting methods.

15.1 Data to be Backed Up

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s), as well as these servers operating systems and logs. It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
- Logs and configuration of network devices such as switches, routers, etc.
- Information stored on employee desktops if the administrator deems such information necessary and backup facilities exist for such an endeavor. The administrator may instead choose to backup a standard desktop configuration and restore data from the file server at his or her discretion.

15.2 Backup Frequency

- **Incremental:** Everyday
- **Full:** Every Friday

15.3 Backup Retention

When determining the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements.

Incremental Backups must be saved for 2 weeks.
Full Backups must be saved for 4 weeks.

16.0 MOBILE COMPUTING POLICY

The mobile computing policy applies to all DICABS employees and staff provided with a company laptop or portable electronic device. It is the employees' responsibility for the proper care and use of the laptop computer / PED (Portable Electronic Device), data and accompanying software while using the same.

16.1 Authorization

Those remotely accessing information systems, data or services containing sensitive or confidential information must be authorized to do so by an appropriate authority, usually the Functional Heads.

Use of computing equipment off campus

Computers or other devices should only be used off-campus for DICABS related activities if DICABS-approved security controls are in place. This provision applies to all equipment, irrespective of ownership. If sensitive or confidential information is being stored or accessed from off-campus, only the member of staff concerned should use the equipment, unless the highest levels of security are in use and an approved access solution, such as via RDP, VPN is used. No sensitive or confidential information is to be stored on any I.T. System that has not been approved by the DICABS.

16.2 Travelling

Portable computing or storage devices are vulnerable to theft, loss or unauthorized access when travelling. DICABS-approved mobile device management software must be installed and activated at all times. Devices must be provided with an appropriate form of access protection such as a password or encryption to prevent unauthorized access to their contents. In addition, more recent means of authentication such as Touch-ID or Face ID are also acceptable forms of access protection.

Equipment and media should not be left unattended in public places and portable devices should be carried as hand luggage. To reduce the opportunities for unauthorized access, automatic shutdown features should be enabled. Passwords or other similar security tokens for access to the DICABS's systems should never be stored on mobile devices or in their carrying cases. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorized persons.

Export and import controls apply when travelling to certain countries which restrict the use of encrypted devices. Advice should be taken from IT Support before any travel arrangements are made.

17.0 LOGGING AND MONITORING POLICY

17.1 Event Logging and Monitoring

Adequate monitoring controls to detect attacks and unauthorized access to its information processing systems must be implemented. The level of monitoring required shall be determined by risk assessment and any relevant or applicable legal requirements shall be identified to ensure that the monitoring activities comply with the requirements. Monitoring may consists of activities such as the review of:

- Automated intrusion detection system logs.
- Firewall logs.
- User account logs.
- Network scanning logs.
- Application logs.
- Help desk tickets.
- Vulnerability Scanning.
- Other log and error files.

Any security issues discovered will be reported to the IT Security Department for investigation.

17.2 User Monitoring

In order to maintain the security of the Group's IT systems (including the network, computers, telephones, and other IT equipment) and the data held on them, the DICABS reserves the right to monitor the use of its IT systems. This may include the monitoring of:

- Internet access and web browsing.
- Email and instant messaging.
- Telephone calls.
- Use of applications.
- Access to files and folders.

Monitoring will be carried out only where there is a legitimate business reason to do so, and it will be conducted in accordance with the DICABS's policies and procedures and any applicable laws and regulations.

18.0 ENCRYPTION POLICY

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the use of encryption.

18.1 Data Storage Devices

All data storage devices that contain sensitive or confidential information must be encrypted using an approved encryption method. This includes, but is not limited to:

- Laptop computers.
- Desktop computers.
- Portable electronic devices (e.g. USB drives, external hard drives, etc.).

- Mobile devices (e.g. smartphones, tablets, etc.).
- Backup media (e.g. tapes, disks, etc.).

18.2 Encryption Administration

The DICABS's IT department is responsible for the administration of encryption technologies and the management of encryption keys. All encryption keys must be stored securely and backed up in accordance with the DICABS's backup and recovery policy.

18.3 Data Transmission

All sensitive or confidential data transmitted over public networks (e.g. the Internet) must be encrypted using an approved encryption method. This includes, but is not limited to:

- Email attachments.
- File transfers.
- Remote access sessions.
- Web-based applications.

18.4 File Encryption

All sensitive or confidential files stored on portable electronic devices or transmitted over public networks must be encrypted using an approved encryption method.

18.5 Encryption Standards

The DICABS shall use only encryption algorithms that have been approved by recognized standards bodies (e.g. NIST, ISO, etc.). The use of proprietary or non-standard encryption algorithms is prohibited.

18.6 Encryption Key Management

All encryption keys must be managed in accordance with the DICABS's key management policy. This includes the secure generation, storage, distribution, and destruction of encryption keys.

19.0 WIRELESS SECURITY POLICY

Wireless networks must be secured to prevent unauthorized access to the DICABS's network and data. All wireless access points must be configured in accordance with the DICABS's wireless security policy.

- All wireless networks must use strong encryption (e.g. WPA2 or higher).
- The use of open or unsecured wireless networks is prohibited.
- All wireless access points must be registered with the IT department and configured in accordance with the DICABS's security standards.
- The use of personal wireless access points within DICABS premises is prohibited.

20.0 SECURITY AWARENESS

All employees must receive regular security awareness training to ensure that they understand their responsibilities for protecting the DICABS's information assets. The training shall cover topics such as:

- The DICABS's information security policies and procedures.
- The importance of protecting sensitive and confidential information.
- The risks associated with the use of IT systems and how to mitigate them.
- How to recognize and report security incidents.

21.0 ONLINE BANKING CHANNELS SECURITY

All online banking channels must be secured to prevent unauthorized access and fraud. The following controls must be implemented:

- Multi-factor authentication must be used for all online banking transactions.
- All online banking activities must be logged and monitored for suspicious activity.
- Employees responsible for online banking must receive specialized training on the risks and controls associated with online banking.

22.0 NEW TECHNOLOGY ADOPTION

22.1 Cloud Computing

The use of cloud computing services must be approved by the IT department and must comply with the DICABS's security policies and procedures. All cloud services must be assessed for security risks before they are adopted.

22.2 Social Media

The use of social media for business purposes must be approved by the DICABS's management. Employees must not disclose sensitive or confidential information on social media platforms.

23.0 COMPLIANCE

23.1 Compliance with Regulatory Requirements

The DICABS shall comply with all applicable laws, regulations, and contractual obligations related to information security.

23.2 Compliance with Information Security Policy and Procedures

All employees must comply with the DICABS's information security policies and procedures. Non-compliance may result in disciplinary action, up to and including termination of employment.

24.0 INFORMATION SYSTEMS AUDIT

The DICABS's information systems shall be subject to regular internal and external audits to ensure compliance with the information security policies and procedures. The results of these audits shall be reported to the DICABS's management and shall be used to improve the DICABS's information security posture.