INFORMATION SECURITY POLICY

Message From The CEO

"At Centrelocus, we think that good security requires the participation and support of all of us as users who interact with data and information systems. It is our own obligation to be aware of these rules and to perform our operations in accordance with them. It is vital to protect firm information as well as the systems that gather, process, and preserve this information. Information system security must contain controls and protections to counter potential threats, as well as measures to assure data confidentiality, integrity, availability, as well as data privacy. The Centrelocus Information Systems Security Policy outlines the procedures for establishing and enforcing our information technology security programme at Centrelocus. Please make sure you are comfortable with our Information System Security Policies"

- **Amit Gupta**

(CEO of Centrelocus)

TABLE OF CONTENT

1. INTRODUCTION – General Overview

1.1. Policy Objectives

The main objectives of this Policy are:

- To define the general security policy for Centrelocus Information Systems and the information stored, processed and transmitted by them, including outsourced services;
- To define a uniform approach, ensuring a high degree of information systems security throughout Centrelocus;
- To define responsibilities with regards to information systems security

This document defines the general framework deriving to specific security policies and system specific security standards, as well as departmental/local procedures. All derived security policies, standards, guidelines and procedures shall be consistent with the present policy document.

1.2 Scope of the Policy

This policy applies to all Centrelocus staff, assignees and contractors that provide services to Centrelocus and is an integral part of the Centrelocus Business Code of Conduct. This policy covers the security of information systems and data networks owned or used by Centrelocus as well as the information that is stored, transmitted or processed by those systems. This policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by Centrelocus.

2. POLICY

This policy is intended to help you make the best use of the computer resources at your disposal, while minimizing the cyber security risks. You should understand the following:

- You are individually responsible for protecting the equipment, software and information in your hands. Security is everyone's responsibility.
- Identify which data is non-public, which includes company confidential data, client data and personal data as further described below. If you do not know or are not sure, ask. Even though you cannot touch it, information is an asset, sometimes a priceless asset.
- Use the resources at your disposal only for the benefit of Centrelocus.
- Understand that you are accountable for what you do on the system.
- Protect equipment from loss & theft. Only store company data on encrypted devices.
- Do not bypass established network and internet access connection rules.
- Do not bypass or uninstall your virus checking or firewall software.
- Do not change or install any unauthorized software or browser 'plug-ins'.
- Do not copy or store Centrelocus data on external devices or unauthorized external locations (including cloud-based services which are not company approved services). Contact IT for the best solution for secured file transfer when this is required.
- If you become aware of a potential or actual Security Incident, you must report the incident as soon as possible by sending an email to: hello@esrotlabs.com

The Policies and supporting Standards in this chapter must be read, understood, acknowledged and followed by all Staff. These set the ground rules under which Centrelocus operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents.

2.1. Data Protection

Centrelocus takes the protection of personal data seriously and the security measures set forth in this policy are essential to ensure the data protection standards supporting the Centrelocus Information Management Policy are met.

2.2. Human Resources Security

(i) Job definition and resourcing

Information security must be covered in the Group's Security Human Resources policy and standards. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; that personnel are adequately screened, trained and that confidentiality agreements are signed by all new employees and contractors.

(ii) User training on Security Awareness

A training plan and training material must be in place to ensure that the right level of Security Awareness is created and maintained within the organization. Software developers and all other relevant personnel involved in the development of software for Centrelocus are required to undertake secure development training on a periodic basis.

2.3. Asset Management

Centrelocus uses a variety of information assets, ranging from laptops and mobile phones to servers. An inventory needs to constantly be maintained and must include the following details for all significant information assets belonging to, or used by the company:

- Asset name and characteristics
- The information owner

- The custodian of the information, and repository location (database etc.)
- The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
- Requirements for the asset regarding availability, uptime, business continuity, etc.

2.4. Hardware Management

At Centrelocus we take a hardware lifecycle approach to hardware management:

- Hardware should only be acquired from approved vendors;
- Only approved software configurations should be applied to new hardware;
- End-users should take appropriate care with any hardware that has been issued to them;
- Lost/Stolen hardware should be reported immediately;
- End-of-Life hardware should be securely disposed.

2.5. Information Management

(i) Information Classification

The Centrelocus Information Security Policy focuses on the protection of the 3 components of information stored on Centrelocus systems: Confidentiality, Integrity & Availability, whilst ensuring Data Privacy. All Centrelocus information must be classified based on these 3 categories in order to allow implementation of the appropriate levels of protection in line with its criticality and to ensure that the controls applied to it are sufficient, and do not impair the company's business. Information classification requirements are detailed in the Centrelocus Information Management Policy.

(ii) Information Handling

Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

- Ensure confidentiality agreements are in place before sharing data externally
- Check email addresses prior to sending any files.
- Files should only be copied to removable storage when necessary and the storage should be encrypted.
- Use restricted access storage areas whenever possible
- Data disposal should be done in accordance with the Information Asset Handling and Protection Standard for End User

2.6. System Asset Policy

Access to information and systems in the possession of, or under the control of Centrelocus must be provided based on a least privilege, need to know basis. All Centrelocus computers must be protected by approved password-based access control systems. Multi-factor authentication for remote access to corporate and production networks by employees, administrators, and third parties shall be implemented where available.

The following rules must be maintained for managing user access rights:

- User registration: approving and granting access rights to users on a need-to-know basis.
- Privilege management. Clear hierarchies must be determined for each system, and each hierarchy must be formally approved.
- User management. As above, each system must have clear procedures for approval and method of granting access to that system. Procedures must exist for each system for joiners, movers and leavers, with audit trails.
- User access rights are subject to periodic reviews.
- Inactive user accounts must be set to automatically disable after 90 days.

2.7. User Authentication Standards

Users must be forced to change their passwords during the first log on, and at 60 - day intervals. Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions. Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the re-use of passwords. A maximum of six successive login failures shall result in account lockout until an administrator unlocks it. Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

(i) Password Selection

In order to make it harder to guess or steal your passwords please keep in mind the following:

- Do not use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first things tried when guessing your passwords.
- Instead try to use acronyms relevant to you only, mnemonics, random letters, etc., and insert no alphabetic characters in the middle of the word
- Use a mixture of UPPER and lower case, numbers and special characters.
- When changing passwords, change more than just the number.
- However, choose something you can remember. It is no use having a strong password if you have it written on a Post-It Note on your desk! If you must have a reminder or hint, use something cryptic that only you can understand.
- Never tell anyone else your password or allow them to log in as you.
- Try to avoid letting other people watch you key-in your password. Choose something that is not easy to guess from watching

- Be aware of 'social engineering'. These are practices used to obtain personal information such as passwords, account numbers etc. (via fake web pages, e-mails, phone calls).
- Phishing is an example of social engineering. Phishing are e-mail messages that entice recipients to divulge passwords and other information (e.g., via clicking embedded links). These e-mails are disguised to appear as if coming from a trusted source. In such cases, do not respond and report this as a Security Incident.
- Use Multi-Factor Authentication, if available. This is a combination of something you know (e.g., password), something you have (e.g., a token, a smartphone) and / or something you are (e.g., biometric – fingerprint).
- Follow all requirements included in the Centrelocus User Authentication Standard.

2.8. Acceptance Use Policy

Corporate IT resources may only be used for Centrelocus business related purposes. You can find the detailed requirements in the dedicated policy named Centrelocus Acceptable Use Policy.

(i) Email Usage

E-mail is a business communication tool which all Centrelocus employees are requested to use in a responsible, effective and lawful manner.

(ii) Internet Usage

Centrelocus provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information. Occasional and limited personal use of the Internet is permitted if such use does not:

- Interfere with work performance & productivity;
- Include downloading or distribution of large files;

- Have negative impact on the performance of Centrelocus' IT systems.

When using Internet access facilities, you should comply with the following guidelines:

- Keep your personal use of Internet to a minimum.
- Check that any information you use from the Internet is accurate, complete and current.
- Respect the legal protections of data, software, copyright and licenses.
- Immediately inform the Security team of any unusual occurrence.
- Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Do not use the company's equipment to make unauthorized access to any other computer or network.
- Do not represent yourself as another person.

It is **STRICTLY FORBIDDEN** to upload Company non-public Information such as any of the following to external file transfer or storage sites, like Box, Drop box or Google Drive:

- Source Code, object code, user documentation and all other software development details. Project related information.
- Personally Identifiable Information.
- Company strategy and business plans.
- Corporate IT infrastructure arrangements including any log files.
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets.
- Employee personal information such as salaries, appraisals, medical records or health care details.
- Any information concerning our clients and prospects including details of our client projects, client proposals, contracts, fees or strategic plans.

- Information related to our clients' customers, including any details stored within Centrelocus software products, such as transaction or bank account details.
- Any other company non-public information.

(iii) Portable Media

The use of portable media is not permitted. The intended purpose is to protect customer and company information from being transferred via unauthorized means. Centrelocus reserves the right to inspect and erase portable media that is used on our network.

2.9. Remote Access and Electronic Communication

Frequently users will be required to access the Group's Information systems from outside the office, for example travelling consultants and/or employees working in Sales / Business Solutions.

For remote access to the Corporate IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used (i.e., Centrelocus Secure Access Portal). The associated security policies must be applied.

Online Communication within Centrelocus offices to an external party may only use Centrelocus approved communication channels. Personal internet connections or connectivity devices (e.g., using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) are strictly prohibited. The detailed Electronic Communication Requirements are described in the dedicated policy named Centrelocus Network and Communications Policy.

2.10.System Changes and Configuration

Centrelocus recognizes that change is a necessary process in order that we can maintain, protect, and enhance services provided to Clients; however uncontrolled change can create significant security risks for Centrelocus. Centrelocus also recognizes that there are different types of change; therefore, an efficient change

management process must be implemented to handle these different types in the most appropriate manner. All changes must be conducted in a controlled and approved way, in accordance with the IT Change Management Standard and IT System Configuration Standard. System changes or re-configurations of standard IT components are not allowed. Only additions and/or changes of software components can be made by users on workstations based on customer project requirements. The following system changes are strictly prohibited

- Installation of Unauthorized connectivity devices (e.g., data modems);
- Any component suitable to gain unauthorized access to restricted areas;
- Any other non-standard software or hardware component.
- Merging of two networks by physically integrating them on a network node;
- Disabling virus protection.

2.11.Network and Communication Policy

(i) Internet Usage

As a part of a global network, we believe securing network is critical to the security of our business:

- External facing networks should be firewalled to an appropriate level
- Physical and logical network changes should only be made by approved users
- Networks should be segregated on a geographical and/or business line basis
- Appropriate controls should be in place at network interfaces
- WAN services should only be acquired through approved vendors
- Network event logging and monitoring should be implemented
- Third-party users shall not connect their computing devices to the wired or wireless network of Centrelocus, unless authorized.

- Centrelocus computers and networks may be connected to third-party computers or networks only with explicit approval after determination that the combined systems will be in compliance with Centrelocus security requirements.

(ii) Wireless Networks

- Passwords for Guest wireless networks should be changed on a regular basis
- Only approved wireless access points should be used
- Wireless networks should always be encrypted

2.12.Threat and Incident Management Policy

(i) 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 consist 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 Information Security Department for investigation. Our detailed policy is set out in the Security Event Logging and Monitoring Standard.

(ii) User Monitoring

In order to maintain the security of the Group's IT systems (including to prevent cyber security threats) and to protect the Group's assets and data, Centrelocus' monitors many aspects of user behavior including but not limited to:

- Monitoring Internet access usage;
- Reviewing material downloaded or uploaded via the Internet;
- Reviewing e-mails sent or received by users, if there is a well-founded suspicion about a breach of provisions of this Policy or of applicable laws, or if there is a legal or regulatory requirement in this respect;
- Reviewing installed software on user's computers;
- Logins to and use of Centrelocus' network as well as use of PCs. Any monitoring done by Centrelocus will be in accordance with applicable law.

2.13.Workstation Security

Workstations include laptops and desktops:

- All workstations should have corporate-approved antivirus software installed and enabled

- All workstations should have data loss protection software installed (where available) ▪ All laptops should be encrypted
- Only install software from trusted sources
- Do not allow unauthorized users to access your workstation
- Take appropriate steps to maintain the physical security of your workstation

2.14.Mobile Device Security

Every mobile device capable of accessing Centrelocus information shall be enrolled in the company MDM solution. In the event of the loss of a mobile device or unauthorized access to a mobile device, the user should contact the local IT team and report the Security Incident to Information Security Team.

Only Centrelocus owned devices are considered trusted and can be connected directly to the Centrelocus Local Area Network (LAN). All non-Centrelocus owned devices are by default considered as untrusted. Untrusted devices must never be connected directly to Centrelocus Internal network, neither through a network cable connection in a Centrelocus office, nor through the Centrelocus Employee wireless network. Untrusted (non - Centrelocus owned) devices are only allowed to use Visitor network access while in a Centrelocus office. Employees' personal devices are not allowed to be connected to CENTRELOCUS corporate network.

2.15.Business Application Management Policy

At Centrelocus we have a high dependency on software to conduct our day-to-day business:

- Applications should comply with the Privacy By Design principle.
- A Data Privacy Impact Assessment (DPIA) should be completed for major software changes that involve personally-identifiable information (PII).
- Security requirements for software should be documented as part of the development process

- Software changes should be subject to change control procedures
- Only authorized users are permitted to deploy software changes This policy only applies to software we develop for internal users e.g., Oracle E-Business, development of the Centrelocus Product Suite is outside the scope of this policy.

2.16.Licensing

Centrelocus uses software from a variety of third parties, copyrighted by the software developer and, unless expressly authorized to do so, employees do not have the right to make copies of the software. The Centrelocus policy is to respect and adhere to all computer software copyrights and to adhere to the terms of all software licenses to which Centrelocus is a party. Also, the Centrelocus policy is to manage its software assets and to ensure that Centrelocus installs and uses only legal software on its workstations and servers, in line with the detailed requirements from the IT Asset Management Standard for Software.

2.17.Encryption

Encryption is required to be used to protect Company nonpublic Information from being disclosed to unauthorized parties. All personnel are responsible for assessing the confidentiality level of data being sent or residing on the devices they use. If data is non-public, all Centrelocus employees are responsible to comply with the Encryption Standard.

2.18.Backup

Centrelocus IT Service Continuity (DR) Policy provides a framework for ensuring that information in scope of this policy will not be lost during an incident affecting availability or integrity. Similarly, all media containing backups of Centrelocus data must be protected according to the data classification related to Data Confidentiality, Integrity & Availability, whilst ensuring data privacy. Both data classification and backup requirements must be determined by the asset owner

and communicated to IT for implementation. Asset / data owners are responsible to inform Corporate IT in writing of the specific backup requirements for each asset or data set and of the required backup retention period in line with IT Service Continuity (DR) Policy.

2.19.Third Party Risk Management Policy

Third Party Risk Management policy defines requirements for carrying out an IT activity with an outsourcer, including Cloud Computing. The process and controls needed to reduce the risks associated with IT outsourcing initiatives, including Cloud Computing arrangements, are detailed in the Centrelocus IT Outsourcing Policy. Centrelocus IT Outsourcing Policy applies equally to all Centrelocus employees and contractors who use an external IT Service provider.

2.20.Malware Protection

A process must be maintained to ensure that malicious software cannot enter the group's secure IT environment. This will include regular anti-malware updates, schedule malware scans and monitoring of events and incidents related to malware, detailed in Centrelocus Threat and Incident Management Policy.

2.21.Business Continuity Management

Centrelocus maintains a group Business Continuity Management Policy (BCMP). This requires sub-functions to develop detailed business continuity plans under its umbrella. The IT function must ensure that the Business Continuity Plan adequately addresses business continuity of the group's IT environment. Disaster recovery planning (DRP) Disaster recovery plan is a subset of BCP. Given the importance of this aspect of the BCP, the key attributes of a disaster recovery plan are discussed below.

There are various categories of disruptive events covered by our BCP/DRP:

- Loss of data, which may include loss of program and system files;

- Unavailability of computer and network equipment.
- Environmental disasters
- Organized/deliberate disruption
- Loss of utilities/services
- Equipment/system failure
- Pandemics
- Cyber Attacks
- Other (health and safety, legal, etc.)

Recovery requirements must be determined by the asset owner based on the criticality of the processes of the Business Functions that use the IT systems (determined through Business Impact Analysis).

The asset owner will ensure the following:

- Sufficient documentation of each Disaster Recovery Plan, needed to enable efficient execution of the plans.
- Disaster Recovery Plan which specifies the appropriate security measures to ensure the degree of confidentiality and integrity required for the recoverable systems.
- That the Disaster Recovery Plan specifies a regular procedure for making copies of data from which to recreate originals in case of a disaster. Disaster backups should not be used for operational recovery.
- The Disaster Recovery Plan must be tested on a periodic basis.

2.22.Physical Security Policy

Access to every office, computer machine room, and other Centrelocus work areas containing sensitive information must be physically restricted to those people with a need to know. Every Centrelocus user must ensure that no important information asset shall be left on desks unattended, especially during non-work hours. At Centrelocus our security is dependent on the physical security of our resources at purpose-built data centers and at on-premise computer room:

- Critical server rooms must be located in a place where the risk of natural disasters is within our risk appetite
- All entry points to IT facilities should be controlled with electronic access control mechanisms
- Appropriate environmental controls such as air conditioning and fire suppression systems should be in place
- There must at least be battery backup power onsite with sufficient duration to switch over to diesel power generation. If there is no diesel backup, then there should be 24 hours of battery power.
- Visitor access should be controlled
- Food and drink is not allowed in Centrelocus data centers. Please see the Physical Security Risk Standard for additional information.

2.23.Risk Management Policy

Our Information Security Risk Management framework is key to the way in which we identify and treat Information Security risks. Our approach is centrally managed but depends on regional and divisional support; therefore, Management should be familiar with the Risk Management Policy and of their role within the framework.

2.24.Security Waivers

Security Policies and Standards are developed to provide the company with a set of rules to help meet certain organizational objectives. From time to time there will be a need to consider a time-limited waiver for exceptions to policy; these will only be considered through the Information Risk Acceptance Standard.

3. BREACHES

Breach of this Policy will be taken seriously and may result in disciplinary actions in conformity with the legal and contractual framework, including termination of employment.

Any user disregarding the rules set out in this Policy or in applicable laws will be fully liable and Centrelocus will disassociate itself from the user as far as legally possible. All breaches of this policy must be reported to the respective Manager/Director for appropriate action.

All security incidents whether actual or suspected, must be reported as soon as possible by sending an email to hello@esrotlabs.com