2017

General User IT Policy

IT department

Innodis Ltd

1/1/2017

Contents

1. POLICY STATEMENT 3

2. SCOPE 4

3. POLICIES 5

3.1 PHYSICAL AND ENVIRONMENTAL SECURITY 5
3.2 LOGICAL SECURITY 8
3.3 COPYRIGHTS AND LICENSES 12
3.4 SOFTWARE INSTALLATION 12
3.5 INFORMATION TECHNOLOGY RESOURCES INTEGRITY 13
3.6 UNAUTHORISED ACCESS 16
3.7 INTERNET ACCESS AND EXTERNAL E-MAIL ACCEPTABLE USE POLICY13 17
3.8 POLITICAL, PERSONAL AND COMMERCIAL USE 24
3.9 BACKUP AND RECOVERY 25
3.10 AWARENESS 26

1. POLICY STATEMENT

Each user is required to secure and maintain the confidentiality of all data and at a level that is commensurate with its value and importance to INNODIS as a whole. The policy follows the **C.I.A** principle: namely Confidentiality of the document based on access control, integrity of the information based on the principle of information protection and finally accountability which is based on the value and verifiability of the information provided.

Data and information must be kept secure from the following:

- corruption (incorrect/ unauthorised modification of data)
- loss (incorrect/ unauthorised deletion of data), and
- access (incorrect/unauthorised access to data)

2. SCOPE

This Policy will be enforced within the entire Organisation, and must be examined and accepted by each user. The Policy may only be modified with the CEO's and/or Board of directors and/or Head of IT approval. The Policy creates the framework within which accountability for securing the Organisation's data and information may be defined.

The Policy shall be subject to periodical review and updates to ensure its relevance and completeness. You shall be made aware of all subsequent changes as and when they occur. This policy may be reviewed every 12 months and depending on new business imperatives, it may be reviewed earlier.

3. POLICIES

If any **user** of the Organisation's information resources is found to have purposefully or recklessly violated any of the following policies, he/she will be subject to disciplinary action, including dismissal and/or such legal action as may be deemed appropriate by management.

The computer systems and network of INNODIS are provided **strictly** for **business use** only. Any use perceived to be **illegal, harassing, offensive,** in violation of other company policies, or any other uses that would reflect adversely on INNODIS can be the basis for disciplinary action or legal action. All employees are expected to make use of these systems with the same integrity as in face-to-face or telephonic business operations.

3.1 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security refers to the procedures put in place to restrict access to the network's physical facilities, to protect them against tampering and unauthorised access, physical destruction and theft. It also refers to such procedures which are meant to safeguard the Organisation's IT assets, namely computers, laptops, etc.

1. **Access to server rooms:** Users are not allowed to access the server rooms, unless accompanied by any member of the IT department or after obtaining express permission from the IT Head of department.

2. **Access <u>to Local Area Network components:</u>** Users are not allowed to access or manipulate Local Area Network (LAN) components, such as wiring cabinets, switches and hubs. Only members of the IT department are authorised to do so.

3. **<u>Hardware Maintenance:</u>** Users should take reasonable care regarding the maintenance of their hardware (computers and laptops) and storage devices (USB, CD-ROMS, tapes). Care should be also taken regarding the cleaning of the equipment provided with the use of only approved products.

4. **<u>Physical Restrictions to Laptops:</u>** When leaving their laptops unattended in an open office, users are required to keep them in a locked filing cabinet. Users should either take the keys with them or remit them to the reception at the floor reception desk or lock the laptop operating system via CTRL+ALT+DEL or a screensaver password.

5. **<u>Procedures before leaving office</u>:** The following procedures should be followed before leaving the office:
   - Shut down PCs and laptops
   - Store all backups, laptops, CD Roms, tapes and other storage media in cabinets or cupboards
   - Disconnect laptops from power adapter. (Laptops which remain connected can be a major cause of fire)
   - See 4 above for storage of laptops

6. **<u>Cyclones:</u>** The following steps should be followed by Users in case of a cyclone:
   - **Class I warning in force**. Perform backups of important working files on the server as instructed by the Head of IT;

- Ensure that backups are kept in a protected, dry area that is safe from flooding ((e.g. store on top shelf of cupboard or top drawer of desk, check windows etc).

- Ensure inventory of all IT equipment is up to date and keep inventory in a safe place.

Class 2 warning in force. The following procedures should be followed before leaving the office:

- Ensure that all IT equipment including (servers/UPS/computers) is moved as far away from windows / air vents / air conditioning units as possible to protect from rain;
- Ensure that IT equipment is not placed on the floor but placed instead on a table or raised surface to protect from flooding;
- Shut down server and all other IT devices if possible and ensure the plugs of all IT equipment are removed from their sockets to protect from a power surge

On leaving the office on a Friday or on the eve of a public holiday, should there be any cyclone threat, please anticipate any of the above precautionary measures that may need to be taken before you leave work premises, so that you are not taken unaware during the weekend or the holiday.

Return to work:

Inspect all IT equipment for damage and notify the following people immediately of any damage: IT manager, IT team member or Immediate Superior. Do not switch on any IT equipment that is visibly damaged by water to avoid risks of electrocution. Please contact the above to deal with this issue.

3.2 PASSWORD SECURITY

Using a password is a method of identifying and authenticating users as they attempt to gain access to a computer system or to a confidential document. Passwords must be designed to be unique and difficult to guess.

All users of the Organisation information resources are required to adhere to the password guidelines as set out below.

Users should:

- Protect all confidential documents on the network, computers and laptops. Use a password protected screensaver on all personal laptops. To set up a password-protected screensaver on your laptop, please contact the IT department.
- Take reasonable steps to safeguard the confidentiality and integrity of their passwords. **Passwords should never be shared.**
- Use a password not less than 8 characters in length.
- Change their passwords at least every six months.
- Be advised that an ideal password contains both alphanumeric and non-alphanumeric characters (e.g.INNODISsr98*$#). If, however, users choose a password consisting only of alphanumeric characters, it should be difficult to guess. Guidance on setting passwords are given in Appendix 3. The first letter of each word in a phrase known to the users may be used (e.g. password is "MNIFAILT" which is made up of the first letter of each word in the phrase 'My name is Fred and I like tennis". Alternatively, the last letter or Xth letter of each word may be used.
- Notify the IT department and have their login account deactivated if they intend to be absent from the place of business for a period exceeding 31 days
- Ultimately, password policy for the domain is enforced at server level.

Users should not:

- Include the users' initial, name, or relatives' name in any form in the password
- Use personal information about himself/herself such as national identity number or vehicle registration number

- Use standard words as found in English or other dictionaries (e.g. 'table", “car", 'chair" etc)
- Use names/ initials of colleagues, friends, departments and organisations
- Use dates for special occasions such as anniversaries, birthdays

- Repeat single characters (e.g. 444333)
- Write down their password. However, if more than one user must have access to the password (e.g. passwords for shared files such as a Word or Excel file), the passwords should be noted and stored in a secure location known only to the users of the files concerned
- Communicate their password in any way whatsoever unless under the circumstances described above
- Use their network Login name in any form in their INNODIS network password, be it reversed, scrambled or repeated
- Use passwords previously used during the previous 150 days
- Share their password with their colleagues. However, passwords for multi-user documents may be shared amongst the users of the file. Non-users must not have access to the password
- Try to maliciously obtain passwords of their colleagues
- Leave critical files on PCs found in the common workspace but perform back up on external storage devices/server before leaving
- Install/Use sniffers, keyloggers, crackers, DDOS, hacking, Trojan, virii software on the network
- Change their IP address without authorization
- Coerce, bride members of the IT department to install software on their equipment without express authorization from the head of IT.

Some of the above may amount to criminal offences covered by the Computer Misuse Act 2010 and may be subject to criminal prosecutions.

3.3 COPYRIGHTS AND LICENSES

All users of the organisation information resources must respect copyrights and license agreements to software and other online information.

1. **Copying and Licenses:** Users must not copy any software protected by copyright and/or under license, from the INNODIS network or into the INNODIS network, except as specifically stipulated in writing by the owner of the copyright or otherwise permitted by copyright law.

See Appendix 3 for a list of softwares for which INNODIS currently has a license.

For further information, please contact the IT manager

2. **Copyrights:** In addition to software, all other copyrighted information retrieved from computer or network resources must be used in conformity with any applicable copyright laws.

For guidance on copyright laws, please contact the IT manager. Breaches of copyright laws can be subject to legal action.

3.4 SOFTWARE INSTALLATION

Users must not personally install software onto computers and/or laptops. All software should be installed by or in the presence of staff from the IT department if available. The following should be contacted for the installation of software:

- IT manager
- IT team member

If installation is performed by other people due to the unavailability of the above, the head of IT should be expressly informed, in writing, prior to the installation (use form in Appendix I for notification).

Please contact the IT manager if you have any doubts as to the license component of any software or component of the software being installed.

All users of the Organisation information resources are discouraged from using public domain, freeware or shareware software, which is freely obtainable without a license at minimal or no cost. Should the use of such software be essential to enable staff to complete their business related activities, the head of IT should be expressly informed, by email, of their intention to use such software (refer to Appendix 1 for authorisation request and acknowledgement form).
The following persons will subsequently acknowledge and authorise such use.

- IT manager
- System Administrator

Modification of any software parameters or PC/laptop configuration by users is strictly forbidden. Users are informed that the IT department shall perform reconfiguration of laptops and PCs from scratch on a random basis. Any unauthorised modification or software on user PCs and laptops will therefore be erased.

3.5 INFORMATION TECHNOLOGY RESOURCES INTEGRITY

All computer users are required to respect the integrity of computer based information technology resources, either hardware or software and to help in the proper functioning of the information system.

3.5.1 General Integrity

Under no circumstances may any users of the Organisation's computer resources introduce any software or hardware, onto the Organisation's hardware or network, without prior written authorisation from the appropriate level of management (see Appendix I for written authorisation).

1. Modification and removal of resources: All computer users may not modify/copy or remove any computer equipment (e.g., hubs, mouse, keyboards, screens etc.) or software (e.g., MSOffice, Acrobat Reader, etc.) without appropriate written authorisation (refer to Appendix I for authorisation request and acknowledgement form) from the IT department.

2. Hindering other users' access: All computer users may not hinder the access of other users to the system.

3. Unauthorised or destructive software: All computer users may not develop or make use of software which will tie up the system, disrupt use by other users or grant them access to restricted areas of the system.

3.5.2 Virus Protection

All Organisation computer resources must have procedures in place to detect and destroy viruses. Viruses may 'infect' data by replicating themselves in already created files or simply by deleting information already stored in files.

In order to prevent viruses entering and spreading on the Organisation network, the following procedures must be followed:

1. Software is only to be installed by authorised IT department staff. Disks, CD- ROMs and programs from external sources are not to be used on the Organisation's computing resources (see section 3.4).

2. When the Organisation has installed virus detection and prevention software, all users must comply with the following procedures:
   - Users must always use the latest version of company approved anti-virus software. The anti-virus should be configured to automatically scan for viruses on power-on, be regularly updated and to perform periodic scheduled scans.

   - Any software and document that is to be introduced by users onto the Organisation’s computer system has to be scanned for viruses and disinfected by the latest version of company's approved anti-virus software before implementation on the system.

   - All abnormal files received either by any external storage system or e-mail should under no circumstances be downloaded onto your hard drive. The receipt of such files should be immediately notified to the IT department and they should download the file onto a stand-alone PC. All abnormal executable files (with extension EXE, COM, VBS, BAT, DLL, COM, CAB) received on e-mail should be notified to the IT department.

     Abnormal files include those that satisfy characteristics:

     1. Sender is unknown
     2. File name is unknown
     3. Software used by file is unknown
     4. Does not fit the general sending pattern/characteristics of the sender

Detection of a virus by the user:

Any machine thought to be infected by a virus shall immediately be disconnected from all networks by the user.

- The user should attempt to remove the virus by using the latest version of company's approved anti-virus software.
- If the software cannot remove the virus or the user does not know how to operate the anti-virus software, the user should immediately contact the following persons in the IT department, clearly describing the source, nature and the effects of the virus (if known).
- The computer should not be connected to the network until the IT department can verify that the virus has been removed.

3.6 UNAUTHORISED ACCESS

Users of the Organisation's information resources are required to refrain from attempting to gain, or allowing others to gain unauthorised access to the system.

1. **Abuse of Privileges:** Users of the system may not grant others access to computer resources without prior written authorisation from management. (refer to **Appendix I** for authorisation request and acknowledgement form)

2. **Problem Reporting.** It is the users' duty to report any deviation from the policies and procedures to the IT department.

Alternatively, users can leave a message on the voice mails 1111 or 5846 or 5815. Reporting problems will allow management to update present policies and procedures to cope with security problems as they are identified.

3. **Intruders:** Users must notify the Services manager by telephone of any suspicious, unaccompanied or unknown people on Organisation premises after ascertaining from these people the purpose of their visit.

4. **Suspicious requests:** Users must notify their managers of any suspicious or unusual requests from unknown persons by phone, e-mail, fax (e.g. names or other personal details of INNODIS staff such as birthdays or age etc).

5. **Social Hacking:** No information must be provided over the phone for access password or equipment used.

3.7 INTERNET ACCESS AND EXTERNAL E-MAIL ACCEPTABLE USE POLICY

This Policy applies to all external communications via e-mail or other similar electronic media which relate to the Organisation's business or involve the Organisation's resources or time (external e-mail) - whether the communication forum or medium is the Internet, an on-line service, a third-party computer network, any other similar medium (an external system). Communication addressed by this Policy includes not only routine email messages, but also any attachments to those messages (e.g., a Word, PowerPoint or Excel document), as well as all news postings, file transfers, chat sessions, etc.

3.7.1 Attribution to Firm By Readers

Any Internet communication or external e-mail originating from or traceable to a person representing the Organisation may be construed by others as attributable to the Organisation. For this reason, all Internet communications and external e- mail must comply with this Policy regardless of the intended audience.

3.7.2 Enforcement

Disciplinary actions, ranging from revocation of Internet access to dismissal, may result from the failure to adhere to any Policy terms and conditions.

3.7.3 Internet Access and External E-mail Policies

Business Use Only

- The sending, receipt or other use of external e-mail, and the use of any related Organisation equipment, networks or resources, is generally intended for Organisation business purposes only. In general, users should only access those resources (e.g., FTP servers, Web pages) required to perform the Organisation business function for which they are authorised.
- The same terms and conditions as those covered on section 3 (Policies) apply to external communication
- Personal e-mail accounts or on-line services for personal use should not be accessed from company computers.
- Casual surfing will be restricted during working hours. A log of internet use will be analysed weekly by management.

Client Confidentiality

No client-related information of any kind and no confidential information pertaining to third parties (e.g., suppliers, vendors, alliance partners) shall be sent via the Internet or any other external system to anyone unless the client or other third party has specifically agreed, in advance, to the Organisation's use of the Internet (or the applicable alternative

external system) for confidential communications. Any such agreement by a client or other party should be in writing (paper or fax). It should be signed by an authorised representative of both the Organisation and the other party (e.g., an officer or a manager who represents that. he/she has such authorisation internally), and should indicate any conditions or limitations (e.g., use of encryption) that apply. It should be based on a specific acknowledgment by the other party that we couldn't assure the confidentiality of any information due to the security risks involved with the Internet or alternative external system.

INNODIS Knowledge Capital

Proprietary or confidential materials or information of the Organisation should not be routinely sent over the Internet or other external systems. Users should carefully consider in each case the risks of conveying such information in this manner, especially as the degree of sensitivity or the value of the materials or information increases. Information of this kind would include, but is not limited to, project proposals, specific project reports or work products, computer software code, proprietary software products and other knowledge capital of the Organisation

- Do not send external e-mails regarding legal matters, unless the lawyer with whom you are working approves it in advance with an acknowledgment of the confidentiality and security risks involved.

  Staff should seek management approval before any messages representing the Organisation or a user are posted to the Internet (WWW, UseNet, e-mail), unless otherwise instructed by a manager or partner.
- USB drive and external storage systems will be disabled by default throughout the organization. Any need for access must be made to the IT Department.
- Unauthorized USB devices (e.g. pendrive, smartcard, cellphone, ipod) not approved by management is strictly prohibited. They can be a source of viruses, unwarranted malicious and non licensed files.

Netiquette

Users should follow the guidelines below regarding the proper etiquette while accessing the Internet for any purpose, including that of sending external e-mail. These guidelines will help users utilise the Internet more effectively and efficiently and will aid in protecting the Organisation's reputation.

- Do not send, redistribute, respond to, or post libelous, slanderous, threatening or abusive messages or any messages that may be construed as such.
- Do not send or otherwise participate in chain letters.
- Exercise extreme caution and be extremely selective when subscribing to mailing lists or similar services. Heavy volume mailing lists can generate 50 or more messages per day per user, and can tremendously degrade network performance.
- Some mailing lists are not turned off easily. Make sure you know how to unsubscribe before requesting a subscription.
- Users may subscribe to mailing lists for Organisation business purposes only.
- Sending of or participation in mails to groups within INNODIS should be strictly restricted to business purposes.

  Exercise extreme caution and be extremely selective when downloading files over IM13 (e.g., GIF, MPEG, audio and video files), as this can tremendously degrade network performance and are not normally authorized.
- All attachments to e-mails being sent (internal or external) exceeding 1MB should be zipped to limit use of network capacity.
- All zipped attachments containing confidential information should be protected by passwords.
- Unauthorised sites are blocked by an automated system during working hours 8:00-12:00 and 13:00-16:30. Any attempt at circumvention will be severely dealt with. Any increase of non-work related activities resulting in damage to the network will cause an all hour, all day, or all week enforcement of this scheme.

Security

- Do not enable any program or macro/agent to automatically forward mail to or via the Internet.
- All sensitive confidential attachments should be password-protected before being sent over the Internet.
- Login IDs, passwords, internal network configurations, addresses and system names must never be transmitted in e-mail messages or to anybody or entity.

  Unauthorized attempts to bypass or circumvent any security system are prohibited.
- Users should ensure that the current standard antivirus software is installed on your computer; and that they scan all files attached to incoming external e-mail as well as any files downloaded from an external system (see section 3.5.2).
- Immediately report any communication, system problem or other condition or circumstance that you suspect may indicate a breach of or risk to the integrity, reliability or security of the Organisation's networks or systems. Contact the IT department:
- The Internet is not a secure environment. Do not assume any activity is private unless the session is encrypted. (SSL 128)

Users must not save confidential information on common drives S:\, unless the sub folder is secured.

- Sharing of files must be done via the mail facility or by approved software such as skype or dropbox.
- Report any suspicious activities to the IT department
- Users are urged to install the latest services packs if they connect directly to the network outside the INNODIS premises (e.g. Home). Please query the IT department for any problem related to updated patch.
- The IT/Audit department has to right to query the machine of anyone at any time. Any issues regarding that should be addressed to the IT Manager or the nearest Manager. Any laptop/pc can be subject to random check by the IT and/or Audit department.

- No usage Peer-to-Peer Software such as kazaa, edonkey, torrents etc. will be tolerated.
- Copyright of movies, music and software must be respected within the company.

Professional Image

- Avoid casual or flippant informality in all of your internal and external e-mail communications and Internet communications in public forums. Despite the inclusion of the required disclaimer noted below, these may be construed as statements by the Organisation and therefore should reflect appropriate formality and professionalism
- When communicating by means of e-mail, users must include the following statement on all communications:

Confidential/Privileged Information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, please destroy this message and notify the sender by reply email. Please advise immediately if you or your employer does not consent to Internet email for messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of my firm shall be understood as neither given nor endorsed by it".

Keep in mind that given the ability to redistribute e-mail, you are never assured that it is a one-time, one-to-one communication. There is no way to prevent redistribution and therefore the above disclaimer is of utmost importance

- The use of the company-owned home computer or laptop and their relative connection to and use of the Internet is inappropriate when that use:

- Compromises the privacy of users and their personal data;
- Damages the integrity of a computer system, or the data or programs stored on a computer system;
- Disrupts the intended use of system or network resources;
- Wastes resources that are needed for business use (people, network bandwidth, or CPU cycles);
- Uses or copies proprietary software when not authorized to do so;
- Uses a computer system as a conduit for unauthorized access attempts on other computer systems;
- Uses a government, corporation, or university-owned system for private purposes or for purposes, which are not in the direct interests of the government, corporation, or university;
- Consists of unauthorized and excessive snooping, probing, or otherwise connecting to a computer in a manner that is deemed not to be of an authorised nature;
- Results in the uploading, downloading, modification, or removal of files on any computer in a network for which such action is not authorized.

Other's Intellectual Property

Software must not be illegally obtained by cracking, serial finding, software modifications. Only media files legally obtained from paid services e.g. itunes, playstore, shazaam, beats etc., can be used.

Use of Laptops outside Business Premises

Access to the Internet from a laptop (which remains the property of INNODIS) outside business premises must adhere to all the same policies that apply to use from within company facilities. Employees should not allow family members or other non-employees to access company computer systems.

3.8 POLITICAL, PERSONAL AND COMMERCIAL USE

Users may not use the information resources of the Organisation for political or personal gain.

1. **Political Use:** Users may not use the information resources of the Organisation for political purposes, unless a written authorisation has been obtained (refer to Appendix I for authorisation request and acknowledgement form) from the following persons:
   • IT manager
   • IT team member

Personal Use: Users may not use the information resources of the Organisation for personal use.

Commercial Use: Where not related to Organisation activities, the use of Organisation information resources for commercial purposes is strictly prohibited. Anything on the INNODIS Knowledge Space resources should not be provided to anyone outside the firm without express authorisation of your head of division.

The distribution of business information (e.g., financial performance of INNODIS, INNODIS strategies, INNODIS payroll details etc.) to the outside world by staff should require authorisation from their departmental head.

3.9 BACKUP AND RECOVERY

It is the responsibility of the users of the Organisation information resources to ensure that all critical and valuable data in their possession are made available for backup where appropriate, in accordance with any backup policies and procedures which may exist. For more information on the current corporate back up policies, please contact:

- IT manager
- System Administrator

It is each user's responsibility to ensure that if their data and software is not included in these backup procedures, but if regarded as being critical, it is to be copied and stored safely. This should be done on a regular basis to ensure that a current backup is always available.

Users may utilise the Windows backup facility to back up their documents. It is highly recommended that users supply a password for their backup file. For instructions on how to use this facility, refer to Appendix 5.

The following represents a guide as to what to back-up:

- Contents of hard-drives on servers and PCs/laptops
- Latest versions of applications
- Databases

Some guidelines on back-up policies are as follows:

- Backup of data should be performed on a regular basis that reflects the rate at which this data evolves .
- Backups of documents may be either stored on external storage devices or on users' home directory on the network (i.e. home directory on "Main\Home [H:]) which is backed up daily.
- Users should keep track of the files which they backup, the backup file name and the date of backup .
- Users should regularly perform a dummy restore of their backups to test its integrity.

3.10 AWARENESS

All information resource users must be aware of relevant standards and policies and their purposes.

1. Renewal of commitment: The policy will be revised at least once a year and users will be required to sign the new policy document version.

2. Induction: An awareness program must be included as part of the induction program held for all new employees joining the Organisation.

4.0 Bring Your Own Device.

In view of modernizing the organization, Innodis is striving to bring the current IT policy to 2016 international corporate use and values. As such, we are enabling the use of personal device to read emails. However, to protect the intellectual property rights of the company, a BYOD program will have to be installed on the private device prior to email enablement. For innodis' phones, it is *de facto* enabled. We currently do not enable third party devices on the system without proper authorization which must come from the IT Manager.

Ultimately, these devices will be allowed to a contained area of the network with minimal access. They are all dedicated for internet access. But in view of maintaining a good online record, the device has to be physically scanned before connecting. This will be handled by the cisco-meraki environment.

Devices owned by Innodis will be explicitly permitted on the wireless network e.g. Iphones, Intermec, Android devices.

Failure to comply with the meraki policy will result in immediate disconnection. This will apply to anyone.

Mobile phones using the global internet access must run on the following operating systems: Android, Blackberry, Windows 10 or Apple IOS.

External devices allowed are: Windows 10, Mac OSX, Ipad IOS, Android.

Windows 8.X , Windows XP, Linux and other OSes are explicitly prohibited.

The person using the BYOD system must ask for authorization via the BYOD portal. It will be allocated for a specific time e.g. 1-2 hours.

GLOSSARY OF TERMS:

Data and Information: For the purposes of this document, data and information will be used interchangeably to refer to both the raw, unrefined, unprepared data and the meaningful, organised, grouped data.

The data and information referred to in this document will include the following:

- Both physical and logical data stored on all types of media
- Database components
- Programs
- Transactions
- Data fields
- Passwords
- Reports, and
- System Parameters

Users: For the purposes of this document the term 'user" will refer to anyone who has been given the authority to use the Organisation's computing resources.

Confidential Information : In general, data can be considered to be confidential if its distribution to unauthorised people or to general groups could potentially cause any of the following:

- Damage to the reputation of INNODIS and/ or any of its stakeholders;
- Damage to the strategic position of INNODIS and/or any of its stakeholders
- Financial losses to INNODIS and/or any of its stakeholders

INNODIS stakeholders include any of the following:

- Shareholders
- Clients
- Directors
- Employees

- Partners
- Consultants
- Financers
- Suppliers

Examples of confidential information include the following:

1. specific project proposals or offer documents;
2. specific project reports or work products;
3. methodologies and work programs;
4. information relating to personnel and payroll (INNODIS and clients);
5. computer software codes (INNODIS and clients);
6. proprietary software products (INNODIS and clients);
7. preliminary financial performance information (INNODIS and clients);
8. information relating to strategy and business plans (INNODIS and clients);
9. information relating to planned merger or acquisition activity (INNODIS and clients) other knowledge capital (INNODIS and clients)

This is not an exhaustive list and users are required to use their common sense to assess the confidentiality of information and the degree of care necessary in handling this data.

Server: The main computer, which shares its resources with clients on the network
Local Area Network : a computer network in which computers in close proximity are able to communicate with each other and share resources
Alphanumeric: containing both alphabetical and numerical symbols
Macro: a single instruction that expands automatically into a set of instructions to perform a particular task
Internet: world-wide 'network of networks"
Zipped: a compressed version of the original file
CPU: Central Processing Unit
FTP: File Transfer Protocol - a means to exchange files across a network
Attachments: Files 'attached" to mails for transfer amongst users

Network bandwidth: relates to the capacity with which the network can send data. It is usually measured in bits-per-second.

Snooping: the use of tools to capture data over the Intenet

Probing: the use of software and IP scanning tools over the Internet to determine whether another computer is connected to the Internet

Uploading: the act of sending a file to be stored on a server. These files can later be accessed by other users.

Downloading: the act of transferring a file from a server onto a local disk of a computer. Both types of loading are done by File Transfer Protocol (FTP).

PC /Laptop configuration: Hardware and Operating system settings for examples set up of network card.

APPENDIX 1 – AUTHORISATION REQUEST AND AUTHORISATION FORM

IT Manager INNODIS

I ……. request to have the following IT related facility installed/upgraded.

Date: ----------

Expected Date of Completion: ----------

Approved by: ----------

Date: ----------

Implemented by: ----------

Date: ----------

APPENDIX 2 – SOFTWARE LICENSES

Software for which INNODIS has licenses and will authorize on its network:

For all users:

Microsoft Office STD (2003/2008/2010/2013), Windows XP/Vista/7 OEM/Windows 10, Citrix Client, Winzip, Winrar, Acrobat Reader, Antivirus Mcafee, Any Browser Supported by Oracle R12, Any Java Client Supported by Oracle R12, Microsoft Visio, Microsoft Project.

For Any Laptop Users:

Cisco VPN/Shrewsoft /Cisco Anyconnect

For IT Personnel and some power users:

Oracle Management, Cognos Client, Oracle Support Suite, MSDN Suite, Microsoft Project, Microsoft Visio, TOAD, Scanning software (Epson, Genius etc), Axis Camera, Apple Itune, Blackberry Desktop, Nokia Client, VmWare View/Workstation, Cisco IP Communicator, Intelliadmin, RealVNC, Oracle ODI, Visual Studio, Intermec SDK, Linco, Temperature Sensors readers, Itrack-Gps, Axis

Software which are freeware or open source but allowed on the network:

Winrar, Winzip, Gimp, Adobe acrobat, Dropbox, ICloud, Itune, AllShare, VLC,
DivX, Live, One Drive, CCleaner