The IDU Group
Internet, Email and Information Security Policy

1. Introduction

Computer information systems, Information and networks are an integral part of business within IDU and any of its subsidiaries (hereafter IDU). IDU has made substantial investments in human capital and financial resources to develop, create and maintain these systems, information and networks and the integrity and operation thereof should be protected at all times.

The enclosed policies have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the reputation of the company.
- Comply with changing legislation

2. Condition of employment

Adherence to this Internet, Email and Information Security Policy is a condition of employment. Contraventions of this policy may result in disciplinary action in accordance with company policy and the company's disciplinary code and procedures as set out elsewhere in the: Company Rules and Regulations as well as the Confidentiality and Secrecy Undertaking documents.

3. Administration

The CIO; and duly appointed Responsible Person(s) are responsible for the administration and enforcement of this policy.

4. Contents

The topics covered in this document include:

- Statement of responsibility.
- The Internet and e-mail usage policy
- Computer viruses.
- User accounts and passwords.
- Physical security.
- Software, copyright and license agreements.
- Mobile and Home computing use.

5. Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list the additional specific responsibilities.

5.1. Manager responsibilities

Managers and supervisors must:

- Ensure that all employees are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

5.2. CIO Responsibilities

The CIO must:

- Implement and/or Develop and maintain solutions, written standards and/or procedures necessary to ensure implementation of and compliance with these policy directives.
- Record, Maintain and update a list of all information assets. - This means that it must be known what type of data there is and where it is located within the organisation.
- Make hardware purchases in order to comply with Information Security Policy and technical requirements. This is to be guided by a user requirements specification. These purchases must be done through standard IDU purchase procedures as determined and approved by IDU.
- Test all new equipment before being introducing it into the live environment; this is in order to assure information security.

- Provide appropriate support and guidance to assist employees to fulfil their responsibilities under this directive.
- Ensure that an Uninterruptible Power Supply (UPS) is installed on business critical equipment to ensure the continuity of services during power outages
- Ensure secondary and backup power generators are to be employed on business critical equipment and systems to ensure the continuity of services during power outages.
- Ensure that network cabling, computer systems and associated infrastructure is installed and maintained at acceptable levels and ONLY by qualified technicians.
- Ensure IT Consumables are purchased in accordance with the organisation's approved purchasing procedures with usage monitored to discourage theft and improper use.
- Ensure that, when commissioning outsourced services, the services used are from reputable companies that operate in accordance with quality standards which should include a suitable Service Level Agreement which meets the organisation's requirements and maintains the desired level of Information Security.
- Must keep up to date System Documentation, Hardware documentation and a formal hardware inventory which should be readily available to the staff who are authorised to support or maintain systems
- Ensure that equipment owned by the organisation may only be disposed of by authorised personnel, through approved companies after ensuring that the relevant security risks have been mitigated and all sensitive information has been adequately removed.
- Set access controls at an appropriate level which minimizes information security risks yet also allows the organisation's business activities to be carried out without undue hindrance.
- Ensure system hardware, operating and application software, the networks and communication systems are all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.
- Ensure that access and activity is monitored and errors, log files and alerts are regularly reviewed and corrective action is taken to ensure Information Security levels are maintained.
- Have adequately planned maintenance schedules in place in order to ensure ongoing operations and effective performance, with any hardware or systems changes being tested prior to live implementation.
- Ensure Information security incidents are identified, responded to, recovered from, and reported timeously using an information security incident management process.
- The information security condition of the organisation should be monitored regularly and reported to executive management and its customers .
- A framework for information security governance should be established, and commitment demonstrated by the organisation's governing body.
- Perform Information risk assessments for target environments (eg critical business environments, business processes, business applications (including those under development), computer systems and networks) on a regular basis.
- Establish Staff agreements that specify information security responsibilities, incorporated into staff contracts, and are taken into account when screening applicants for employment.
- Undertake specific activities such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organisation.
-

6. The Internet and e-mail usage policy

The Internet is a large, publicly accessible network of networks that has millions of connected users and organisations world-wide. The World-Wide Web (WWW) is a subset of the Internet and is a collection of interlinked documents and multi-media files.

6.1. Policy

Access to the Internet and e-mail is provided to employees solely for the benefit of IDU and its business operations. Access to both the Internet and e-mail is a privilege and such access is entirely at the discretion of the CIO or his specific assigned delegates. Employees are able to connect to a variety of business information resources around the world, through the WWW. Internet access through the company network is limited to company employees and others that the company may authorise from time to time.

Conversely, the Internet and WWW is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the company's interests the following policy has been established for using the Internet and e-mail.

The reasonable private use of e-mail and Internet is accepted but must be kept to a minimum, and not breach company policy. The company will not accept any liability regarding the use of the Internet or e-mail facilities when used for private use.

6.2. Acceptable use

Employees using the Internet including e-mail are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using web browsers to obtain business information for company use from commercial or academic web sites.
- Accessing databases for information as needed for company business.
- Using e-mail for business contacts.
- Utilising the Internet, including e-mail, as a tool to advance the business objectives of the company.
- E-mail will be considered a valid form of communication on par with written communication

6.3. Unacceptable use

Employees must not use the Internet or e-mail for purposes that are illegal, unethical, harmful to the company (including statements, actions or omissions that do, or could, lead to civil and/or criminal liability to the company or damage or loss to the company or its reputation) or fellow employees. Examples of unacceptable use are:

- Sending unsecured sensitive personal information pertaining to the company, its suppliers, customers or staff is prohibited.
- Viewing, accessing, copying, processing or transmitting of any content or material that is offensive, harassing, fraudulent, illegal or obscene including any form of pornography, hate mail, racist or sexist remarks or hoaxes to any company employee, trading partner, customer or anybody else.
- Sending or forwarding chain or unsolicited ("spam") e-mail, for example, e-mail messages containing instructions to forward the message to others where not for official or company business purpose (chain letters).
- Sending or forwarding personal information, joke e-mails, electronic greeting cards, Christmas cards, music files (e.g. MP3), video clips (not related to official business) and games may be blocked and/or removed from the system at the discretion of the CIO.
- Sending large e-mails is discouraged and is only to be done for specific work purposes.
- Representing personal opinions as that of the group company via e-mail or publication of unauthorised statements onto web sites, bulletin boards, discussion areas or newsgroups.
- Conducting a personal business using company resources.
- Conducting any form of a campaign that maybe considered as damaging against fellow employee/s or any third party by e-mail.
- Using third party e-mail providers not approved and provided by IDU, i.e. "Hotmail", "Gmail", "Yahoomail", "Freemail" or any other e-mail service provided by an outside Internet Service Provider or party, this is strictly prohibited on IDU equipment. This is prohibited because it allows for the unsecured transmission of company information or any files emanating from within the company to external parties.
- Using an Internet file storage facility such as "Dropbox", "Skydrive", "Google Apps", "Xdrive", "Netdrive", "DiskOnNet", etc., to make backups or copies of files from the company onto the Internet. The IT manager should provide adequate facilities for the employee to store and make backups of crucial working files in company authorised facilities. Use of such internet storage facilities will only be allowed where it is required for specific work purposes and with the written consent of the CIO or his assigned representative.
- Providing computing or storage resources, including file/disk sharing or swapping, to external parties through file sharing and torrent type websites and services. This activity is strictly prohibited.
- Using a modem whilst connected to the company's internal network – under no circumstances is any modem allowed to be used when a workstation or laptop is connected directly to the company's network.
- Opening of unsolicited or spam emails - Unsolicited mail must not be opened; it should be deleted and reported immediately to the CIO.

6.4. Employee responsibilities

Company employees may access the Internet through the company's network for the primary purpose of conducting the company's business. Viewing, copying, storing or sending Internet content outside of the scope of the company's employment must be kept to a minimum. The company provides Internet access through the company's network to company employees as a privilege that is based on adherence to the company's policies and rules regarding Internet access.

In addition to being responsible to abide by the conditions as set out in this end-user policy, including but not limited to this paragraph an employee who uses the Internet or Internet e-mail shall:

- Ensure that communications not interfere with his/her or any other employee's productivity.
- Be responsible for the content of all text, audio, or images that he/she stores on his/her machine or places on or sends over the Internet.
- Not transmit copyrighted materials without permission of the author thereof and/or without defining and acknowledging the owner thereof.
- Know and abide by all applicable IDU policies dealing with security and confidentiality of company records.
- Avoid, where possible, transmission of confidential information of the company or its stakeholders. If it is necessary to transmit confidential information, employees are required to take steps to ensure that information is delivered to the proper person who is authorised to receive such information for a legitimate purpose using the most secure channel available.
- Report any form of irregularity or transgression of this end-user policy to the company CIO.
- Only authorised employees shall engage in talking to the press, placing or publishing information on the Internet, other than the sending or receiving of e-mail. Employees shall observe all existing standards, policies and regulations regarding materials published on the company's behalf and shall establish accountability for all information regarding the company's business or publications posted on the Internet for public access.
- Ensure that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons.

6.5. E-mail identification & disclaimer

To ensure that an e-mail message is properly identified, apart from the sender's e-mail address it is compulsory that all emails sent from IDU has the following e-mail signature applied at the foot of each individual e-mail message. No changes are permitted without the written acceptance of the CIO.

* Replace the text between the brackets [ ] with the required information, personal mobile numbers are optional:

[EMPLOYEE NAME]
[JOB TITLE]

T +27 (0) 21 [OFFICE NO]
C +27 (0) [MOBILE NO]
Teams +27 (0)[TEAMS NO]

[email address]
www.idusoft.com

NOTE: This signature may be automated and the addition of internet, marketing and social media links will be updated as required to conform to business requirements.

6.6 Copyright & Downloads

Employees using the Internet are not permitted to illegally and/or wrongfully copy, transfer, rename, add, modify or delete protected works, information or programmes. Employees are responsible for observing copyright and licensing agreements that may apply when downloading or distributing files, documents and software. Any copyrighted material attached to a message should identify the author and acknowledge his/her copyright.

Employees must obtain approval from the CIO before downloading any material including material for which a fee is requested. Failure to observe copyright or license agreements may result in disciplinary action being taken against the employee by the company and/or legal action by the copyright owner.

6.7. Monitoring & Privacy

All Internet communications, including e-mail, created, sent, or retrieved on IDU equipment and infrastructure is regarded as company information, and the company reserves the right to intercept, read and inspect the same if the company believes, in its sole judgement, that it is justified to do so in order to protect its business and ensure compliance with this and other policies of IDU. IDU provides Internet access and e-mail facilities to assist Users in performing their job. With due regard to the South African Constitution and the Regulation of Interception of Communications Act, ECT Act and Protection of Personal Information Act, in order for the company to effectively manage its electronic communication resources and information security compliance requirements the following rules apply:

- There are a wide variety of contents available on the Internet other than that which a User may use for work. Accessing the Internet for non-IDU purposes on company time and/or with company equipment must be kept to a minimum and must not breach any company policy.
- IDU reserves the right to record the location of all Internet sites accessed by Users, files or videos viewed, files downloaded and email communication and attachments sent and received on company time and/or equipment. IDU reserves the right, in its sole discretion, to share this information or make public a complete listing of all sites visited by the Users to any requesting party to the extent permitted or required by law.
- IDU reserves the right to block Users from any Internet resources, including but not limited to those which IDU determines in its sole discretion to have no legitimate IDU purpose or which could have detrimental impact on IDU's computing resources or reputation.

Each employee has given his or her consent, or shall be deemed to have given such consent, for his or her activity to be monitored if he or she uses the company's computers for network activity, access to the Internet or to send e-mails.

The company shall respect the employee's right to privacy as far as is reasonably possible, subject to the protection of the company's rights and interest in and to its business.

The monitoring of user activity, including document access, e-mail(s) and internet activity will only be undertaken by specific staff assigned to perform this task by the CIO. Access to user related files including, but not limited to, documents, e-mail(s), internet and activity log files will only be performed by these assigned individuals and will only be done with the informed consent and approval of the CIO.

Furthermore, the staff assigned to monitor activity and enforce this policy will maintain the highest level of confidentiality. This in turn will ensure the appropriate measures for information security and employee confidentiality are maintained.

All communications, including text, video or audio clips and images, can be disclosed to law enforcement agencies or other third parties without prior consent.

7. Computer viruses

Computer viruses are programmes designed to make unauthorised changes to programmes and data. Therefore, viruses can cause destruction of corporate resources. It is important to know that computer viruses are much easier to prevent than to cure. Defences against computer viruses include protection against unauthorised access to computer systems, using only trusted sources for data and programmes, and maintaining virus-scanning software.

7.1. CIO Responsibilities

The CIO shall:

- Install and maintain appropriate anti-virus software on all computers and ensure that anti-virus updates are sent regularly to employees.
- Respond to all virus attacks, destroy any virus detected and document each incident.

7.2. Employee responsibilities

- Employees shall not knowingly introduce a computer virus into company computers.
- Where anti-virus updates are not automatically received from the CIO, it is the employee's responsibility to ensure that the updates are run as soon as possible after receiving such updates.

- Run a virus scan on any executable file(s) received through e-mail.
- Employees shall not load diskettes, CD-ROMS, DVDs, USB Flash Disks, external hard drives or any other media type of unknown origin. All incoming media shall be scanned for viruses before they are read or executed. Any external devices or media can only be loaded onto the IDU network with the approval of the CIO.
- Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY remove the network cable or disconnect from the network and POWER OFF the workstation and notify the CIO who will take corrective action.

8. User accounts and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorised employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

In addition employees shall access the Internet in a manner that does not compromise the company's network security. This includes the employee keeping their username and password secure, prohibiting access to intruders or viruses, and report any suspicious activity to the company's CIO. Employees that want to download Internet content from non company sources must observe company security procedures and first gain CIO approval.

8.1. CIO Responsibilities

The CIO, or his duly appointed representative shall be responsible for the administration of access controls to all company computer systems. The CIO will process additions, deletions, and changes to hardware, configurations and systems upon receipt of a written request from the employee's manager.

Deletions may be processed by an oral request prior to reception of the written request. The CIO will maintain a list of administrative access codes and passwords and keep this list in a secure area.

8.2. Employee responsibilities

Each employee:

- Shall be responsible for all computer activity and transactions that are made with his/her User ID (username) and password.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded or kept where they might be easily obtained.
- Shall use passwords that will not be easily guessed by others. A minimum length of 6 (six) characters are required for a password and must contain at least one (1) special character.
- Shall lock the screen, log out (or shutdown) when leaving a workstation. In the circumstance where these options are not available the user must ensure that a screensaver is used that is protected by a password that automatically activates after a maximum of 10 (ten) minutes of inactivity on the computer screen.
- Using a workstation, PC or laptop is to ensure that their screens are clear / blank when not being used.

8.3. Manager/Supervisor's responsibility

Managers and supervisors should notify the CIO promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked or revised. Involuntary terminations must be reported concurrent with the termination. The termination of access rights is at the discretion of the relevant line/department manager.

8.4. Human resources responsibility

The Personnel/Human Resources Department of the company will notify the CIO of associate transfers and terminations immediately.

9. Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, fraud, unauthorised access, and environmental hazards.

9.1. Employee responsibilities

The policy below applies to all employees:

- Diskettes/media, documents and files shall be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up in lockable cupboards, filing cabinets or a safe and are never to be left in the open.
- Diskettes/media shall be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Other environmental hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold should be avoided.
- Since the CIO, or his duly appointed representative, is responsible for all equipment installations, disconnection, modifications, and relocations, employees are not to perform these activities. These activities are ONLY to be performed by qualified technicians with the appropriate management planning and approval.
- Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their department manager and CIO. Informed consent means that the manager knows what equipment is leaving, what data is on it and for what purpose it will be used.
- Employees shall exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty will be accountable for any loss or damage that may result. Each employee is responsible for the security of their assigned equipment.
- Under no circumstance may any other equipment be connected to the company's network without prior, written approval by the CIO. This includes laptops, PDA's, USB Memory Sticks, MP3 Players, Smart Phones, Tablet Devices, etc
- Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible. Both the owner of the information and the intended recipient must authorise the transmissions in writing beforehand
- Sensitive or Confidential Information may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing. This includes company information as well as personal employee information e.g. salary printouts, customer data or any other information deemed to be of a personal nature such as Identity Documents, Credit Card details, etc. This policy also applies to photocopying of sensitive information; this information must never be left in the open.
- Personnel issued with mobile phones by the organisation are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed.
- Sensitive or confidential information must not be recorded on any answering machine/voice mail systems.
- Personnel using business centres to work on the organisation's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business centre's systems. This activity is discouraged and must only be done when absolutely necessary and other options are not available.
- All information system hardware and software faults are to be reported promptly and logged in the call logging system. These calls are ONLY to be resolved by authorised and adequately qualified personnel.
- Only suitable and approved cleaning materials are to be used on equipment owned by the organisation.
- Deliberate or accidental damage to organisation property must be reported as soon as it is noticed.
- Staff using company mobile phones, company credit cards, company petrol cards OR Fleet management cards are responsible for their security and responsible use.
- Ensure that all sensitive and confidential information is stored securely on a server and not on the local machine.
- An Employee must never divulge sensitive or confidential information to anyone who is not authorised to receive it. This information includes company information and that of fellow employees. The recipients of this information include, but are not limited to; family, friends, competitors, customers or suppliers.

10. Software copyright and license agreements

All software acquired for or on behalf of the company or developed by company employees or contract personnel on behalf of the company is and shall be deemed company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

Non-compliance with legislation dealing with intellectual property, including copyright, such as the Copyright Act and with license agreements can expose IDU and the responsible employee(s) to civil and/or criminal liability. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of law.

This policy applies to all software that is owned by IDU, licensed to IDU, or developed for IDU by employees or third party vendors.

10.1. CIO Responsibilities

The CIO shall:

- Maintain records of software licenses owned by IDU.
- Periodically scan company computers to verify that only authorised software is installed.

10.2. Employee responsibilities

Employees shall not:

- Install software unless authorised by the CIO. Only software that is licensed to or owned by IDU is to be installed on IDU computers. Under no circumstances will any assistance/support be given on unauthorised or illegal products.
- Copy software unless authorised and recorded by the CIO.
- Download and install software unless authorised by the CIO.

10.3 Developing and Maintaining Software

The following policy applies to software development:

- Only designated staff may access any software development libraries. Amendments may only be made using a formal change control procedure.
- All changes to programs must be properly authorised and tested before moving to the live environment.
- Program listings must be controlled and kept fully up to date at all times.
- Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.
- Emergency amendments to software are to be discouraged, except in circumstances previously designated by management as 'critical'. Any such amendments must strictly follow agreed change control procedures.
- The use of live data for testing new systems or system changes may only be permitted where adequate controls for the security of the data are in place.
- All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available
- All development of software must use robust version control and ensure that versions and changes are adequately backed up.

11. Mobile and Home computing usage

Please note that this section of the policy applies to any employees who are eligible for a laptop, personal digital assistant, tablet, company mobile phone, data card or equivalent mobile device used to access the company's network or information resources whilst travelling or from home or any other location outside of the office. Employees who carry and use mobile devices are at risk – particularly if they are unaware of common sense security measures which should be adopted to protect mobile devices and their content from theft and unauthorised data access.

11.1. CIO Responsibilities

The CIO shall:

- Explain to the employee the relevant risks associated with mobile devices in terms of physical protection and access to information stored on the device.
- Ensure that the necessary backup facilities are provided to the employee.
- Provide guidance in the use of the mobile device to the employee when travelling abroad – especially as it relates to communications, electricity supply and foreign support.
- Ensure that remote access control procedures provide adequate safeguards through robust identification and authentication techniques.
- Permanent staff, temporary staff and contractors are to be made aware of the Information Security policy in place at IDU, and training should be provided where necessary.
- Ensure the mobile devices, laptops, storage devices or equivalent are encrypted to ensure data protection;

11.2. Employee responsibilities

Employees shall:

- Ensure that access to the information contained on the mobile device will be protected by a minimum of a password into the operating system and screen savers. Where possible, ensure that a further level of encryption for business related information is put into place by means of the device's operating system or any other similar application.
- Ensure that under no circumstances any unauthorised user is allowed to use this facility. This includes lending the device or handing over physical possession of the device to an unauthorised party.
- Ensure that when the company's network is accessed from home or during a business trip that the necessary security software that will establish secure communication to the company's security systems is utilised. Assume that when travelling abroad all communications are intercepted and recorded.
- Time spent online interacting with company systems should be limited and done for a specific purpose.
- Take care when travelling, especially in aircraft, buses or any other mass transport, that external parties could easily read information off screens. Employees should therefore exercise the necessary caution when working on company related information in public or non-company areas and ensure that the screen is clear/blank when not in use.
- When travelling by aircraft, bus or any other means of mass or public transport, ensure the device is carried as hand luggage and not checked in.
- When staying in hotels make certain that the device is locked in the hotel's safekeeping and not left unattended in the hotel room.
- Make sure that the carry case and device is clearly identified by taping contact details onto it, for example by taping a business card onto the back of the device. Other methods of identifying the device are encouraged.
- Make sure that if you are unable to take the device with you it is locked away from sight when left in a vehicle, for example in the vehicle's boot – including when travelling. This does not include extended periods such as overnight, and then the device shall be stored securely outside the vehicle.
- Make backups of crucial files on the device, according to IDU Backup procedures, and store it separately from the device and on the company's server.
- Not save any passwords or access codes anywhere on the device. This includes taping notes onto the device or keeping it inside the carry case of the device.
- Not leave the device in direct sunlight or where it is exposed to any other environmental hazards such as dust, liquids, chemicals and food. In the event that liquid is spilt onto the device, attempt to drain all excess liquid – DO NOT TURN THE DEVICE ON. Return it to the CIO as soon as possible. Do not use household chemicals or water to clean the device – use only a dust cloth.
- Attempt not to drop or knock the device. Perform a regular check on the condition of the strap of the carry case and the carry case itself.
- In the event of a mobile device being stolen, immediately report the theft to the company IT Manager to arrange for all security access to be suspended.

12. IDU Customer Security

Special mention must be made in connection with the networks, systems and information of IDU's customers. Various employees, in the course of performing their job function at IDU, will have access to the networks, systems and information of IDU's customers. This will occur for many reasons; these reasons include, but are not limited to Maintenance, Consulting, Upgrades, support, etc. In the course of business all of the same policies mentioned in this document will apply to IDU's customer's networks, systems and information.

The same level of care, confidentiality and responsibility for conduct is expected from all employees of IDU as if they were performing their work on IDU's own infrastructure. It must also be noted that this policy does not replace or take precedence over any policy or procedure which is in place at IDU's customer's sites. The rules and responsibilities as laid out in this document are there to provide enhanced protection of IDU's customer's infrastructure.

If there are any aspects regarding this policy that are unclear please consult with your CIO.

Acknowledgement of the
IDU Internet, Email and Information Security Policy

This form is used to acknowledge receipt of, and agreement with, the IDU Internet, Email and Information Security Policy.

Procedure
Complete the following steps:

- Read the "IDU Internet, Email and Information Security Policy".
- If applicable complete the section on mobile and home computing usage.
- Sign in full and complete the details in the spaces provided below.
- Return this acknowledgement form to your CIO.

Mobile and home computing usage
I hereby acknowledge receipt of the following mobile computing device handed to me by the company for the purposes of utilizing the same in the course and scope of the performance of my duties. I understand that I will be held personally responsible for any specified financial loss sustained through any negligence on my part if the equipment listed is damaged or stolen.

Make & Model	
Serial Number	
Processor	
Memory	
Hard drive	
Comments	

Signature
By signing below, I agree to the following terms:

- I have received and read a copy of the IDU Internet, Email and Information Security Policy and understand the same;
- I understand and agree that any computers, software, and storage media provided to me by IDU contains proprietary and confidential information about IDU and its business and remains the property of the company at all times;
- I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at IDU), or otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
- I agree that, if I leave IDU for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, storage media, sensitive information or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control;
- I agree to abide by the terms set out in the IDU Internet, email and Information Security Policy and to be bound thereby. In particular, I understand and accept that IDU may monitor and access the information, data and e-mail on my computer;
- I understand and agree that failure on my part to comply with the terms as set out in the IDU Internet, Email and Information Security Policy and this acknowledgement form may result in disciplinary action being taken against me.

Employee signature: _____

Employee name: _____

Department: _____ Date: _____