# INFORMATION SECURITY POLICY

City Integration Limited

## Last Revision Date

25 September 2018

## Document Owner

Christian Wells

# Table of Contents

## Document History

| Date | User | Section | Content | Version |
|---|---|---|---|---|
| 25/09/2018 | CW | All | Document Creation | v1.0 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | |
|---|---|
| City Integration Limited | **Policy and Procedure** |
| **Title: INTRODUCTION** | **P&P #:** IS-1.0 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Introduction

### Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at City Integration Limited, hereinafter, referred to as the **Company**. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Company with policies and guidelines concerning the acceptable use of Company technology equipment, e-mail, Internet connections, voicemail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Company employees or temporary workers at all locations and by contractors working with the Company as subcontractors.

### Scope

This policy document defines common security requirements for all Company personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Company, entities in the private sector, in cases where Company has a legal, contractual or fiduciary duty to protect said resources while in Company custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Company network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Company in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Company domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Company at its office locations or at remote locales.

## Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

**CEO –** The Chief Executive Officer is responsible for the overall privacy and security Company's of the company.

**CIO** – The Chief Information Officer

**Employee –** A permanent or temporary resource engaged by the company. For the avoidance of doubt this includes Contract staff and persons engaged to the Company through third parties.

**Encryption** – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

**External Media –i.e.** CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

**FAT –** File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

**Firewall –** a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

**FTP** – File Transfer Protocol

**IT** - Information Technology

**LAN** – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.

**NTFS –** New Technology File Systems – NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

**SOW - Statement of Work -** An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

**User** - Any person authorized to access an information resource.

> **Privileged Users –** system administrators and others specifically identified and authorized by Company management.
>
> **Users with edit/update capabilities –** individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**
>
> **Users with inquiry (read only) capabilities** – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

**VLAN –** Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

**VPN** – Virtual Private Network – Provides a secure passage through the public Internet.

**WAN** – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national, international.
**Virus -** a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

## Objectives

The objectives of the Information Security Policy of the Company is to:

- Reduce the Risk of IT problems
- Plan for and deal with IT issues as and when they arise
- Keep working if there are problems
- Protect information relating to the Company, Employees and Clients
- Keep valuable proprietary company information that may have commercial value safe and secure
- Meet legal requirements for Information Security
- Allow employees to operate within a secure environment where they are aware of their obligations
- Safeguard Information of Clients of the Company

## Goals

To identify through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk.
To manage the risks to an acceptable level though the design, implementation and maintenance of a formal Information Security Management System.
To comply with legislation including;

- Companies Act (2006)
- Health and Safety at Work Act (1974)
- Interception of Communication Act (1985)
- The Data Protection Act (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- General Data Protection Regulation (2018)

To comply with any customer contract conditions relating to information security.
Commitment to comply with ISO 27001-2013 (Information Security Management).

## Responsibilities

- Christian Wells is the Director with overall responsibility for IT security.
- Max Cantello has day to day responsibility for implementing the Information Security Policy and is the assigned Information Security Officer.

- Clarion Communication Management Limited – IT Supplier to the Company including cloud networks and IT security systems.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: EMPLOYEE RESPONSIBILITIES** | **P&P #:** IS-1.1 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Employee Responsibilities

### Employee Requirements

The first line of defence in data security is the individual Company user. Company users are responsible for the security of all data which may come to them in whatever format. The Company is responsible for maintaining ongoing training programs to inform all users of these requirements.

Protection of Data

It is the responsibility of the employee to ensure that data belonging to the Company and Clients of the Company is used in a responsible manner, is not distributed and that all reasonable measures are made to protect data and other IT assets that are used in the course of business.

Wear Identifying Badge so that it may be easily viewed by others **-**

Where the Client provides the employee with Identification Badges in order to help maintain building security, all employees should prominently display their employee identification badge. Other people who may be within Company facilities should be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel **-** It is the responsibility of all Company personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Company office location, you should challenge them as to their right to be there. All visitors to Company offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Company. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop with a Cable Lock **-** When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers.

Most Company computers will contain sensitive data and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while travelling. The cable locks are not foolproof, but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Company Corporate Assets - Only computer hardware and software owned by and installed by the Company is permitted to be connected to or installed on Company equipment. Only software that has been approved for corporate use by the Company may be installed on Company equipment. Personal computers supplied by the Company are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Company for home use.

Equipment supplied by the client may only be used outside of the client premises in accordance with the client policy.

Retention of Ownership - All software programs and documentation generated or provided by employees, Company's, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Company employees at their own expense.

## Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

  Exception: Authorized information system support personnel, or others authorized by the Company , may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The wilful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Company computers must be approved by the Company.

- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.

## Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, The Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voicemail, instant messaging, Internet, fax, personal computers, and servers.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not pre-empt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Company information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Company information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Company premises. The Company encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.
    e) Harassment – The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-colour jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company’s equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialled, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Company reserves the right, at its discretion, to review any employee’s files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

## Internet Access

Internet access is provided for Company users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Company should not be used for entertainment, listening to music, viewing sports, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Company routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

## Reporting Software Malfunctions

Users should inform the appropriate Company personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Company computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel as soon as possible. Write down any unusual behaviour of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

## Report Security Incidents

It is the responsibility of each Company employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately.

Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the Company to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Company shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police.

## Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Company and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Company policy and will result in personnel action, and may result in legal action.

## Internet Security

Employees must familiarise themselves with risks and threats posed by online access and should review Get Safe Online: https://www.getsafeonline.org/

## Transferring Software and Files between Home and Work

Personal software shall not be used on Company computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Company purchased software on home or on non-Company computers or equipment.

Company proprietary data, including but not limited to information relating to clients of the Company, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Company without written consent of the Company or Client. It is crucial to the Company to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Company data to a non-Company Computer System, the supervisor or department head should notify the  or appropriate personnel of the intentions and the need for such a transfer of data.

The Company Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Company does not control non-Company personal computers, the Company cannot be sure of the methods that may or may not be in place to protect Company sensitive information, hence the need for this restriction.

## Internet Considerations

Special precautions are required to block Internet (public) access to Company information resources not intended for public access, and to protect confidential Company information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Company shall be obtained before:

- An Internet, or other external network connection, is established;

- Company information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the Company. The network can be used to market services related to the Company, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Company or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

**Installation of authentication and encryption certificates on the e-mail system**

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

**Use of WinZip encrypted and zipped e-mail**

This software allows Company personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Company staff member who desires to utilize this technology may request this software from the or appropriate personnel.

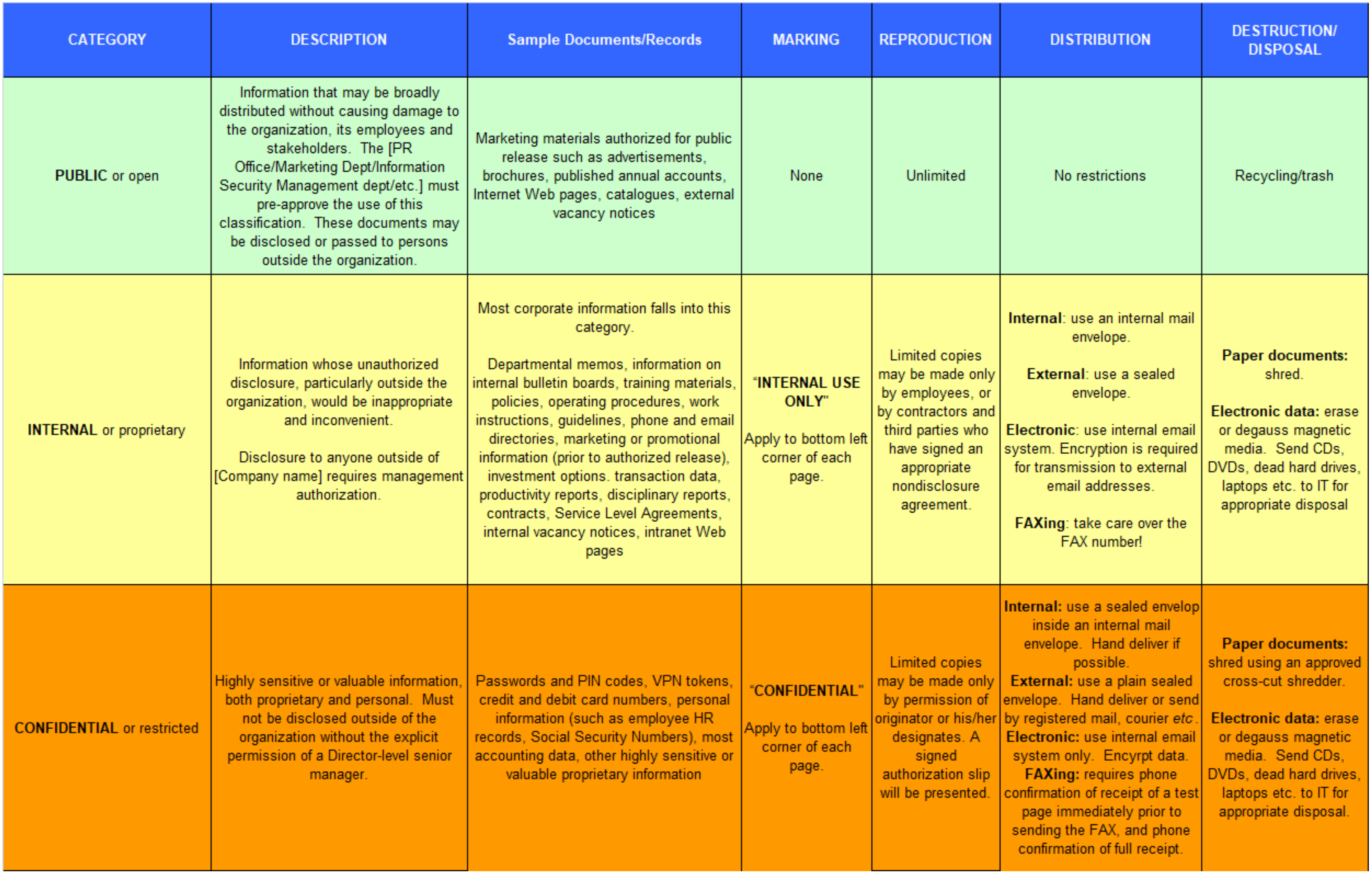
**Back Up and Disaster Recovery**

Company data is backed up on a daily basis.
Each week a set of back up data is transferred offsite and stored securely.
The form performs a Disaster Recovery test each year.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: INFORMATION CLASSIFICATION** | **P&P #:** IS-1.1b |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Information Classification

Information is classified and must be treated as per the table below:



| CATEGORY | DESCRIPTION | Sample Documents/Records | MARKING | REPRODUCTION | DISTRIBUTION | DESTRUCTION/ DISPOSAL |
|---|---|---|---|---|---|---|
| **PUBLIC** or open | Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. The [PR Office/Marketing Dept/Information Security Management dept/etc.] must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization. | Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices | None | Unlimited | No restrictions | Recycling/trash |
| **INTERNAL** or proprietary | Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient.<br>Disclosure to anyone outside of [Company name] requires management authorization. | Most corporate information falls into this category.<br>Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options. transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages | **"INTERNAL USE ONLY"**<br>Apply to bottom left corner of each page. | Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement. | **Internal**: use an internal mail envelope.<br>**External**: use a sealed envelope.<br>**Electronic**: use internal email system. Encryption is required for transmission to external email addresses.<br>**FAXing**: take care over the FAX number! | **Paper documents:** shred.<br>**Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal |
| **CONFIDENTIAL** or restricted | Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager. | Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information | **"CONFIDENTIAL"**<br>Apply to bottom left corner of each page. | Limited copies may be made only by permission of originator or his/her designates. A signed authorization slip will be presented. | **Internal:** use a sealed envelop inside an internal mail envelope. Hand deliver if possible.<br>**External:** use a plain sealed envelope. Hand deliver or send by registered mail, courier *etc*.<br>**Electronic:** use internal email system only. Encyrpt data.<br>**FAXing:** requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt. | **Paper documents:** shred using an approved cross-cut shredder.<br>**Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal. |

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: IDENTIFICATION and AUTHENTICATION** | **P&P #:** IS-1.2 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Identification and Authentication

### User Logon IDs

Individual users shall have unique logon ids and passwords. An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use/misuse of their individual logon id.

All user login ids are audited at least twice yearly and all inactive logon ids are revoked. The Company HR department notifies the ISO upon the departure of all employees and contractors, at which time login ids are revoked.

The logon id is locked/revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Company systems or networks must have a completed and signed Network Access Form (Appendix A). This form must be signed by the supervisor or department head of each user requesting access.

### Passwords

#### User Account Passwords

User ids and passwords are required in order to gain access to all Company networks and workstations. All passwords are restricted by a corporate wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.
Reuse - The previous twelve passwords cannot be reused.
Restrictions on Sharing Passwords - Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.
Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.
Passwords or PINs must not be written down
Multiple use of Passwords - Passwords must only be used for a single application. The same password must not be used for more than one application.

### Confidentiality Agreement

Users of Company information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix B). The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the COMPANY information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Company information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

### Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Form.

### Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: NETWORK CONNECTIVITY** | **P&P #:** IS-1.3 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Network Connectivity

### Dial-In Connections

Access to Company information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialling without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the  or appropriate personnel.

### Dial Out Connections

Company provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the  or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place

### Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the  or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- mobile phones

- Smartphone devices
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- telephone equipment

### Permanent Connections

The security of Company systems can be jeopardized from third party locations if security Company's and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Company systems. The or appropriate personnel should be involved in the process, design and approval.

### Emphasis on Security in Third Party Contracts

Access to Company computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Company Information Security Policy have been reviewed and considered.
- Policies and standards established in the Company information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Company computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance

should be understood and agreement upon in advance.

- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.
- Security policies of Clients of the Company must be adhered to at all times.

### Firewalls

Authority from the  or appropriate personnel must be received before any employee or contractor is granted access to a Company router or firewall.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: MALICIOUS CODE** | **P&P #:** IS-1.4 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Malicious Code:

### Antivirus Software Installation

Antivirus software is installed on all Company personal computers and servers. Virus update patterns are updated daily on the Company servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

> Configuration **-** Antivirus software is implemented by the Company and is constantly upgraded to the latest release. It is the responsibility of the Employee to ensure that devices supplied by the Company are upgraded.
> Remote Deployment Configuration **-** Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.
> Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Company network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the or appropriate personnel.

### New Software Distribution

Only software created by Company application staff, if applicable, or software approved by the or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Company computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Company hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Company computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Company personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Company computer or network.

Computers shall never be “booted” from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not “bootable”.

## Retention of Ownership

All software programs and documentation generated or provided by employees, Company’s, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Company ownership at the time of employment. Nothing contained herein applies to software purchased by Company employees at their own expense.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: ENCRYPTION** | **P&P #:** IS-1.5 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Encryption

**Definition**

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

**Encryption Key**

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Company shall establish the criteria in conjunction with the  or appropriate personnel. The Company employs several methods of secure data transmission.

**Installation of authentication and encryption certificates on the e-mail system**

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the  or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

**Use of WinZip encrypted and zipped e-mail**

This software allows Company personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Company staff member who desires to utilize this technology may request this software from the  or appropriate personnel.

**File Transfer Protocol (FTP)**

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the  or appropriate personnel.

## Secure Socket Layer (SSL) Web Interface

Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have appropriate approval from the supervisor or department head as well as the  or appropriate personnel before any access is granted.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: BUILDING SECURITY** | **P&P #:** IS-1.6 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Premises Security

It is the policy of the Company to provide building access in a secure manner. Each site, if applicable, is unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Company strives to continuously upgrade and expand its security and to enhance protection of its assets and confidential information that has been entrusted to it. The following list identifies measures that are in effect at the Company. All other facilities, if applicable, have similar security appropriate for that location.

Description of building, location, square footage, and the use of any generator.

- The Premises of the Company have a Private Entrance and is accessed by a Chubb key.
- The Company has designated several keyholders. It is the responsibility of the keyholder to ensure that the premises are secured when there are no Employees on the premises.
- Any unknown or unauthorised persons entering the premises must be immediately challenged, including persons claiming to be doing work on the premises such as cleaners or maintenance staff.
- Employees must ensure that when not in use all documentation is stored in lockable fireproof cabinets provided by the Company.
- Employees must use their utmost discretion when handling sensitive information and documentation and must not share this information with other persons including colleagues unless there is a business need to do so. In the case of doubt the Employee must refer to a Director of the Company or authorised person of a Client
- Employees must be acquainted with and fully respect building security relating to Clients

| City Integration Limited | Policy and Procedure |
|---|---|
| **Title: TELECOMMUTING** | **P&P #:** IS-1.7 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Company considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Company office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Company network or Client network where authorised by the Client, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Company's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

Any Telecommunicating performed on behalf of a Client must be done in full compliance of the Client procedures and is only permitted where authorised by the Client.

### General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

## Required Equipment

Employees approved for telecommuting must understand that the Company will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

### Company Provided:

Company supplied workstation.
A cable lock to secure the workstation to a fixed object.
If using VPN, a Company issued hardware firewall is required.
If printing, a Company supplied printer.
If approved by your supervisor, a Company supplied phone.

### Employee Provided:

Broadband connection and fees,
Paper shredder,
Secure office environment isolated from visitors and family,
A lockable file cabinet or safe to secure documents when away from the home office.

## Hardware Security Protections

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Company personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing Company information of any type. The Company requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

## Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate Company personnel for assistance. Protect external media by keeping it in your possession when travelling.

Transferring Data to the Company**:** Transferring of data to the Company requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Company.

External System Access: If you require access to an external system, contact your supervisor or department head.  or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information via e-mail unless it is encrypted.  If you need assistance with this, contact the  or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Company Networks: Extreme care must be taken when connecting Company equipment to a home or hotel network. Although the Company actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Company has no ability to monitor or control the security procedures on non-Company networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces.  If your laptop has not been set up with an encrypted work space, contact the  or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area.  Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies.  Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Company**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement.  Do not give or transfer any patient level information to anyone outside the Company without the written approval of your supervisor.

## Disposal of Paper and/or External Media

Shredding:  All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Company work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with Company procedures.

- Do not throw any media containing sensitive, protected information in rubbish bins.
- Return all external media to your Manager or to the Client
- External media must be wiped clean of all data.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

| | |
|---|---|
| City Integration Limited | **Policy and Procedure** |
| **Title: SPECIFIC PROTOCOLS AND DEVICES** | **P&P #:** IS-1.8 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Specific Protocols and Devices

### Wireless Usage Standards and Policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Company employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Company laptops and mobile devices.

Approval Procedure **-** In order to be granted the ability to utilize the wireless network interface on your Company laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the  or appropriate personnel of the Company. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by appropriate Company personnel to setup your laptop and schedule training.

Software Requirements **-** The following is a list of minimum software requirements for any Company laptop that is granted the privilege to use wireless access:

- Antivirus software
- Full Disk Encryption

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

Training Requirements **-** Once you have gained approval for wireless access on your Company computer, you will be required to attend a usage and security training session to be provided by the  or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

## Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Company in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Company networks. Every workstation or server that has been used by either Company employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Company data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Company employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common Company within the Company. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Company networks. Transportable media received from an external source could potentially pose a threat to Company networks. ***Sensitive data*** includes all human resource data, financial data, Company proprietary information.

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Company data or sensitive data must be an encrypted USB key issued by the  or appropriate personnel.  The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Company.
- Non-Company workstations and laptops may not have the same security protection standards required by the Company, and accordingly virus patterns could potentially be transferred from the non-Company device to the media and then back to the Company workstation.

  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

- Data may be exchanged between Company workstations/networks and workstations used within the Company. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:

  Data provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into Company workstations or servers as long as the source of the media in on the Company Approved Vendor list (Appendix D).
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the  or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves the Company, all transportable media in their possession must be returned to the Company.

The Company utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The  or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Company laptops, workstation, or servers must be wiped of data. Thus all transportable media must be returned to the  or appropriate personnel for data erasure when no longer in use.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE** | **P&P #:** IS-1.10 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Disposal of External Media / Hardware

### Disposal of External Media

It must be assumed that any external media in the possession of an employee may contain sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown into rubbish bins.
- When no longer needed all forms of external media are to be sent to the  or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used.
-

### Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made.  Asset tags and any other identifying logos or markings will be removed.

### Disposition of Excess Equipment

As the older Company computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title:**<br>**Emergency Operations Procedures (EHR outage)** | **P&P #:** IS-2.0 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Information Technology** |

## Emergency Operations Procedures

### Purpose

In the event of systems being unavailable due to planned or unexpected outages the Company will instruct the Employee or Contractor as to what action to take.

### Definitions

Company Management (PM) – A Company Management System is usually a computer based system used to manage the day-to-day operations of a company. Tasks typically performed by a PM system include: scheduling appointments, maintaining client information including contacts, billing functions and generating various reports.

### Procedures

### Notification:

The Company will advise as soon as practicable in the event of:

- planned downtime of systems,
- unexpected outage of systems, and
- resumption of systems following an outage such that normal operations may resume.

### Client sites:

In the event of an outage or system unavailability at a client site the employee should act in accordance with the Client procedures.

| City Integration Limited | **Policy and Procedure** |
|---|---|
| **Title: Sanction Policy**<br>Security Violations and Disciplinary Action | **P&P #:** IS-4.0 |
| **Approval Date: 25 September 2018** | **Review: Annual** |
| **Effective Date: 25 September 2018** | **Human Resources** |

## Sanction Policy

**Policy**

It is the policy of the Company that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Company will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

The Company will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Company's information security and privacy.

**Purpose**

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of Company's security policies, Directives, and/or any other legal regulatory requirements.

**Definitions**

*Workforce member* means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

*Sensitive information*, includes, but not limited to, the following:

- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Company.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Company.
- Financial/accounting records – Any records related to the accounting Company's or financial statements of the Company.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.
- Personally Identifiable Information that allows the identification of real persons
- Financial data relating to the Company or Client's of the Company.

*Availability* refers to data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* refers to data or information is not made available or disclosed to unauthorized persons or processes.

*Integrity* refers to data or information that have not been altered or destroyed in an unauthorized manner.

## Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

| Level | Description of Violation |
|---|---|
| 1 | • Accessing information that you do not need to know to do your job.<br>• Sharing computer access codes (user name & password).<br>• Leaving computer unattended while being able to access sensitive information.<br>• Disclosing sensitive information with unauthorized persons.<br>• Copying sensitive information without authorization.<br>• Changing sensitive information without authorization.<br>• Discussing sensitive information in a public area or in an area where the public could overhear the conversation.<br>• Discussing sensitive information with an unauthorized person.<br>• Failing/refusing to cooperate with the Information Security Officer, Chief Information Officer, and/or authorized designee. |
| 2 | • Second occurrence of any Level 1 offence (does not have to be the same offence).<br>• Unauthorized use or disclosure of sensitive information.<br>• Using another person's computer access code (user name & password).<br>• Failing/refusing to comply with a remediation resolution or recommendation. |
| 3 | • Third occurrence of any Level 1 offence (does not have to be the same offence).<br>• Second occurrence of any Level 2 offence (does not have to be the same offence).<br>• Obtaining sensitive information under false pretences.<br>• Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm. |

## Recommended Disciplinary Actions

In the event that a workforce member violates the Company's privacy and security policies the following recommended disciplinary actions will apply.

| Violation Level | Recommended Disciplinary Action |
|---|---|
| 1 | • Verbal or written reprimand<br>• Retraining on privacy/security awareness<br>• Retraining on the Company's privacy and security policies<br>• Retraining on the proper use of internal or required forms |
| 2 | • Letter of Reprimand*; or suspension<br>• Retraining on privacy/security awareness<br>• Retraining on the Company's privacy and security policies<br>• Retraining on the proper use of internal or required forms |
| 3 | • Termination of employment or contract<br>• Civil or Criminal penalties as provided under national law |

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Company shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behaviour which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

### Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Company.

### Related Policies

Information Security Policy

# Appendix A – Network Access Request Form

## Employee or Contractor Request for Network Access

### EMPLOYEE/CONTRACTOR INFORMATION

□ New Employee □ New Contractor □ Existing User Today's Date:
□ Temporary

First Name: Last Name: *MI:

Position: Director:

□ Full-time □ Part-time

Start date or Requested due date:
Temporary or Contractor end date, if known:

### SECURITY & EMAIL

New Account:
□ Network Account □ Email
□ Security/Email similar to what existing user:

□ Include in which E-mail Group(s): □ Remove from which E-mail Group(s):
□ Include in which Security Group(s): □ Remove from which Security Group(s):

□ Permit access to the following network location(s):
Drive Path Access: □ Read-only □ Read/write □ Full Access □ Remove Access
Drive Path Access: □ Read-only □ Read/write □ Full Access □ Remove Access
Drive Path Access: □ Read-only □ Read/write □ Full Access □ Remove Access

□ Miscellaneous Needs *(Enter any other requests)*:

### HARDWARE & SOFTWARE

Hardware:
□ Laptop □ Desktop □ Either Laptop or Desktop
□ Screen protector □ Laptop bag □ Cable lock
□ Multifunction printer □ Netgear Router □ Numeric keypad
□ Standard inkjet printer □ Dual monitors □ Docking station
□ iPhone □ iPad □ Windows Mobile Device

Software:
□ Adobe Acrobat (full version) □ Email Encryption
□ Microsoft Office Professional □ Microsoft Office Professional
□ MS Project □ MS Visio □ MS OneNote
□ Fax Server

□ Miscellaneous Needs *(Enter any other requests)*:

### TELEPHONY

Telephone:
□ Desk Phone □ Smartphone (IP Communicator)
□ Desk phone currently exist at location. Current extension is:

Accessories:
□ Wireless headset □ Wired headset

### MOBILE PHONE

□ Mobile Phone

Accessories:
□ Mobile Phone Case/Holder □ Car Charger
□ Miscellaneous Needs *(Enter any other requests)*:

### BUILDING ACCESS

Access Requested for the following location(s):
□ Office □ Server Room
□ Lobby □ Other, *Specify:*

Additional Access Restriction:
□ After-Hours Access, *Specify Hours:*

Other Restrictions (be specific):

### SPECIAL INSTRUCTIONS

Manager Checklist/Reminder:

- Signature below can be of the Director or the Data Owner if new network access is requested.
- Ensure employee badge is requested
- Schedule new employee orientation, if applicable
- Ensure name appears on any appropriate sign-in/out sheets
- Remember to have all new employees/contractors read and sign appropriate forms, i.e. Confidentiality Form (Appendix B)
- Request appropriate training/background:
  - HR Background Investigation
  - Security Training
  - Any additional training and/or background check

| **NAME** | **SIGNATURE** | **DATE** |
|---|---|---|
| **Director (Print Name)** | | |
| **Appropriate Authority** | | |

Appendix B – Confidentiality Form

# RESPONSIBILITY OF CONFIDENTIALITY

I understand and agree to maintain and safeguard the confidentiality of privileged information of Company Name. Further, I understand that any unauthorized use or disclosure of information residing on the Company information resource system may result in disciplinary action consistent with the policies and procedures of national law.

Date Signature

Company/Firm

Date Signature of Company

# Appendix C – Approved Software

The following list has been approved for use by the Company. All software must be installed and maintained by the appropriate Company personnel.

| Software | Version | Approved by | Date | Description/Comments |
|---|---|---|---|---|
| Microsoft 365 | | | | Includes Outlook |
| Microsoft Office | | | | Inc. Visio, Project |
| Bullhorn Reach | | | | Recruitment application |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix D – Approved Vendors

| Vendor | Primary Contact | Main Number | Product / Service | Description/Comments |
|---|---|---|---|---|
| Clarion Communication Management | | 0333 222 6635 | IT Hosting | Cloud hosting for Company IT systems.<br>Telecoms systems |
| GoDaddy | | 020 7084 1810 | Web hosting | |
| | | | | |

# Appendix E – Breach Assessment Tool

## PRIVACY BREACH ASSESSMENT

1) Was Private Information Involved? □ Yes □ No

2) Was the Private Information encrypted? □ Yes □ No

3) Description of breach:

a) What data elements have been breached? Personal information, financial information that could be used for identity theft are examples of sensitive personal information.

b) What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

c) What was the date that the breach was discovered? ______________________

d) What is believed to be the date that the breach occurred? ____________________

2) Cause and Extent of the Breach

a) What is the cause of the breach?

b) Is there a risk of ongoing or further exposure of the information? □ Yes □ No

c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

d) Is the information encrypted or otherwise not readily accessible? □ Yes □ No

e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

a) How many individuals are affected by the breach?

1. Who was affected by the breach:

□ Employees

□ Customer-owners

□ Volunteers

□ Contractors

□ Service providers

□ Other individuals/organizations

4) Foreseeable Harm from the Breach

a) Is there any relationship between the unauthorized recipients and the data subject?
□ Yes □ No

b) Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

2. What harm to the individuals will result from the breach? Harm that may occur includes:

□ Security risk (e.g., physical safety)

□ Identity theft or fraud

□ Loss of business or employment opportunities

□ Hurt, humiliation, damage to reputation or relationships

□ Other (please specify):

d) What harm could result to the organization as a result of the breach?

□ Loss of trust in the organization

□ Loss of assets

□ Financial exposure

□ Other (please specify):

e) What harm could result to the public as a result of the breach?

□ Risk to public health

□ Risk to public safety

□ Other (please specify):