

NON-PROFIT GIRLS EMPOWERMENT IN FLORIDA

A photograph of four young women with long hair, smiling and huddled together outdoors. They are wearing casual clothing like plaid shirts, a white t-shirt, and overalls. The image has a soft, warm filter. A red rectangular box is overlaid on the bottom right of the image, containing the text 'IT COMPLIANCE MANUAL' in white.

IT COMPLIANCE MANUAL

[ORGANIZATION] POLICY

Policy Title: INFORMATION SECURITY
AUDIT AND ACCOUNTABILITY
POLICY

Policy #: xxxxxx

Issued by: Business Services

Original Date: xxxxxx

ELT Approval: [Approver's Name]
[Approver's Position]

Revised Date:

PURPOSE

The purpose of this policy is to establish information security standards and ensure proper care and accountability in handling activities that support the processes relevant to Information Technology Resources at [Organization].

SCOPE AND APPLICABILITY

This policy applies to all Users who have access to Information Resources and company equipment at [Organization].

AUDIT AND ACCOUNTABILITY

Auditing Security Logs is part of the monitoring of activities used in a proactive manner to detect and act upon unauthorized access and illegal or unethical use of [Organization] Computer Systems.

[Organization] IT Security reserves the right to monitor and audit any and all activity on its Computer Systems, either routinely as part of breach prevention, system maintenance, system improvement, or suspected violation.

Audit reports of original Security Logs work to strengthen the [Organization] IT System security. For the clarity of the reports and the transparency of relevant log information,

[Redacted]

[Redacted]

[Organization] IT Security reserves the right to trace and audit the actions of

[Redacted]

All Security Logs and audit reports will be retained for the purposes of accountability and the maintenance of effective Information Security at [Organization]. In accordance with our records keeping and related security policies, standards and procedures, we will keep the audit logs for [Redacted] if needed during the investigation of system failure or system

breaches. [Organization] also reserves the right to keep copies of [REDACTED]

IT Security reserves the right to routinely review [REDACTED]

[REDACTED] It may do so periodically to verify that Security Logs are properly secured, or to audit the use of [Organization]'s resources.

Additionally, an automated alert response will be created to [REDACTED]

[REDACTED] IT Security is responsible for ensuring that the system is fully supported with protection mechanisms, and the capacity to take action.

While we recognize that unintentional and human errors are not uncommon, Users should ensure they are following all the policies, in order to minimize these events.

In case of a known unauthorized log-in or awareness of compromised security, any User with such information should report it to [authorized person's email].

It is the responsibility of IT Security to keep the log records and audit reports safe. The audit information will only be accessible [REDACTED]

Audit records are kept for IT Security review and analysis purposes. In case of an investigation into suspicious or unusual system activity, audit records and reports are admissible as evidence.

ENFORCEMENT

Violations of this Policy that come to the attention of [Organization] IT or HR during auditing and other activities will be denied access to Information Resources, and may result in disciplinary action, including termination of employment or pursuit of legal action.

Any User who undertakes on behalf of [Organization] with knowledge of an alleged violation of this Policy shall notify Information Security as soon as possible.

[ORGANIZATION] POLICY

Policy Title: SECURITY OF INFORMATION
TECHNOLOGY EQUIPMENT

Policy #: xxx

Issued by: Business Services

Original Date: xxx

ELT Approval: [Approver's Name]
[Approver's Position]

Revised Date:

PURPOSE

This policy protects [Organization]

POLICY STATEMENT

- [Organization] (Centers, offices, departments, etc.) [redacted]. This is required for all such systems but is especially critical for those systems that support vital business functions and/or host sensitive personal or institutional information.
- Recipients of [Organization] Technology (hardware and software) are responsible for securing it from damage, theft, misuse, and loss.
- [Organization] equipment replacement and upgrades must meet the standards and the approval of the [Organization] IT Department to receive support. [redacted]
[redacted] [Organization] IT Department's established standard model hardware. If a [redacted] sought are above the standard model hardware, [redacted]
- Employees are responsible for equipment [redacted]
[redacted] and software issued to them by [Organization]; and, therefore, shall report any damage, loss, theft or other unauthorized access.
- [Organization]-[redacted] on the employee's signed [Organization] Equipment Issuance Form.
- If a piece of [Organization] IT equipment is damaged, lost, missing, or stolen:
 - [redacted]
 - [redacted]

- Follow the instructions outlined in the following policies and procedures:

Policy BS 8.04-Vehicle/Facility/Liability Incident Reporting;

Policy BS8.11-Inventory Management and Control; and

Standard Operating Procedure SOP1.06-CCC Reporting.

- Access to [Organization] information assets is restricted to authorized individuals and will only to be used for authorized purposes. ■
- All [Organization] ■ must be saved on [Organization] Information Systems approved devices. This includes, but is not limited to, [Organization] ■
- All employees or authorized agents of [Organization] ■ [Organization]) are responsible for protecting and preserving [Organization] equipment and software from misappropriation, misapplication, and conversion.
- All computer systems may be audited or tracked at any time ■
- Any [Organization] employee or authorized agent ■ shall immediately report ■ to a [Organization] Information Technology Representative, Center Executive Director (ED) or ED designee. ■ must be completed immediately and forwarded to the Director of IT or designee.
- Employees are not permitted to allow non-[Organization] employees to use the [Organization]-owned equipment ■ from the [Organization] IT Department.
- Employees are not permitted to connect ■ to the [Organization] internal network. Non-[Organization]- ■ to the [Organization] "Guest Wireless" network or equivalent.
- Any personal or confidential data transferred out of any [Organization] Location to any other Location or to any external destination ■ All internal [Organization] network links are secure links.
- Employees are responsible for reporting any repair issues to the [Organization] IT Department as soon as possible.
- Computing systems which have been ■ at [Organization] to facilitate access and distribution of electronic information for the purpose of conducting organizational activities ■
- If the equipment cannot be repaired or reused, it must be properly handled, not as standard waste ■

- All equipment connected electronically, including computer components, hardware and hard drives must [REDACTED]
- This includes following secure [REDACTED] by electronically disabling, digitally wiping, and restoring "factory settings" on all used equipment, and manually re-configuring settings, de-linking and disabling access to the [Organization] Computer System. [REDACTED]

- **Portable Workstation Encryption**

- As a measure for securing workstations and avoiding data breaches, loss, theft, and misuse, [Organization] [REDACTED]. The primary control for access to information and approval authorization limits are managed [REDACTED]
- Any equipment receiving information should also be monitored carefully whenever sensitive information is being sent or received. [REDACTED] and that sensitive information is not disclosed inadvertently by leaving confidential information unprotected.
- Each user will be accountable [REDACTED] to the IT/Cyber policy requirements.
- Users are fully accountable for all activity within their own account [REDACTED]. This means [REDACTED] the extent prescribed by the agency's confidentiality policies, and refraining from any practice, which might jeopardize the [Organization] encryption system.

- **Patching and Update**

The [Organization] IT Department has the authority and responsibility [REDACTED] Center's IT/Cyber systems.

The IT Department is responsible for:

- [REDACTED] required for the support and implementation of the IT/Cyber Policy throughout the organization;
- recommending update and security directions;
- promptly responding to and investigating [REDACTED]
- reporting [REDACTED] in order to assist in determining overall [Organization] system risk assessment;
- monitoring [REDACTED] with related IT security updates and policies throughout [Organization];

- implementing [REDACTED] and other measures as part of [Organization] activities;
- assisting in patching the effectiveness of information security and compliance with [REDACTED]
- ensuring effective update and use of software and software licenses.

Security is the responsibility of the end user and is mandatory; [REDACTED]
[REDACTED]

PROCEDURES

There are no procedures related to this policy.

[ORGANIZATION] POLICY

Policy Title:	DATA BACKUP POLICY	Policy #:	xxx
Issued by:	Business Services	Original Date:	xxx
ELT Approval:	[Approver's Name] [Approver's Position]	Revised Date:	

PURPOSE

This policy defines the backup procedures to protect data of [Organization] from loss. [REDACTED]

POLICY STATEMENT

- Backup procedures protect data from loss and ensure recovery in the event of an equipment failure, intentional destruction of data, or disaster. • [REDACTED]
- All documents requiring back up must be saved [REDACTED] All information stored on a computer hard drive is not backed up and cannot be recovered if lost or damaged.
- The IT Department will perform regular backups, test backups [REDACTED]
- Users are responsible for ensuring their individual data is saved and backed up. [Organization] IT should be contacted if assistance is needed.
- Users requesting files be restored must submit a request to the IT help desk which will include information [REDACTED]
- Security is the responsibility of the end user and is mandatory. Violation of any provision of this policy and any applicable state and federal regulations and laws may be cause for disciplinary action [REDACTED]
- Sensitive and confidential information must be protected to prevent its unauthorized disclosure. [REDACTED]
- Data stored should be backed up on a regular basis to protect it from loss due to equipment failure or human error. [REDACTED] Backup equipment should be stored in a secure manner, preferably away from the premises where the primary copy of the data is kept.

- To facilitate backup, [REDACTED], not on local workstation, C: drives.
- The data should be [REDACTED], which will also be part of the general data backup procedures.
- Backup of personal data on [Organization] workstations or servers is discouraged. [Organization] [REDACTED] to [Organization] activities be removed.
- Employees who have reason to believe that the [REDACTED] or that [REDACTED] or [REDACTED], misuse of logins or passwords or unauthorized use must report this immediately to the IT Department.
- **Data retention**
 - [Organization] [REDACTED] on the [Organization]-owned equipment and/or network infrastructure in order to assure full compliance with its IT/Cyber policy by all Users who have or have had access to its system.
 - Users should familiarize themselves with activities which [REDACTED] that are subject to data retention.
 - [Organization] also reserves the right to [REDACTED] on [Organization] [REDACTED] [Organization] networks, and may do so periodically to [REDACTED] (such as computer viruses or unauthorized software), or to audit the use of [Organization] resources.
- **Data monitoring**
 - [Organization] has the right to monitor any and all aspects of its computer system, [REDACTED], saved or received by employees.
 - Employees [REDACTED] in anything they create, store, send, or receive on [Organization] equipment.
 - [Organization] keeps a complete list of User access information [REDACTED] [Organization] or otherwise [REDACTED], so that the company can recover the data [REDACTED]
 - Similarly, because unintentional errors do occur, any user of [Organization] Computer Systems that inadvertently finds they have access to information they know they should not have, or are not sure they should have, [REDACTED]

Any violation of this Policy that comes to the attention of the management will be acted upon accordingly, [REDACTED] by the organization.

PROCEDURES

There are no procedures related to this policy.

Copyright – The Write Direction Inc.

[ORGANIZATION] POLICY

Policy Title: COMPUTER SOFTWARE
USAGE

Policy #: xxx

Issued by: Business Services

Original Date: xxx

ELT Approval: [Approver's Name]
[Approver's Position]

Revised Date:

PURPOSE

This policy:

- Ensures that [Organization] employees are properly trained on safe and legal use of [Organization]-owned software.
- Prevents violations of the terms of [Organization] software license agreements [REDACTED] owned by [Organization] or private computers used to perform work related to [Organization].

POLICY STATEMENT

[Organization] employees shall use computer software in compliance with the terms and conditions [REDACTED]

- General

- The [Organization] IT Department purchases and licenses software from a variety of sources. [REDACTED]

- and is [REDACTED]

- Installation of unauthorized software on any device, i.e., computer, tablet, smartphone, or network server within [Organization] is not permitted. [REDACTED]

- [REDACTED]. [Organization] IT reserves the right to remove any unauthorized software from any [Organization]-owned equipment.

- Software Usage Policy

- Only software authorized by [Organization] [REDACTED]

- [REDACTED]. No unauthorized or personally purchased software is permitted on [Organization] devices or its network without prior written authorization from the [Organization] IT Department.

– Personal software, or software that an employee has acquired for non-business purposes, may not be installed on [Organization]-issued devices. [REDACTED]

[REDACTED] on [Organization] [REDACTED]
[Organization] [REDACTED].

– Personal or unsolicited software [REDACTED]
[REDACTED] may not be loaded onto [Organization] equipment as there is a [REDACTED]
[REDACTED]

– [Organization] IT reserves the right to [REDACTED]
[REDACTED] from [Organization]-owned devices.

– Software on [Organization]-owned devices shall only be used [REDACTED]
[REDACTED] for that software.

– Software must be installed by a [Organization] IT representative once the registration requirements have been completed and verified. [REDACTED]
[REDACTED] at the [Organization] [REDACTED]
[REDACTED] IT Department.

– [Organization]-owned software cannot be loaded on a user's home device [REDACTED]
[REDACTED]

– If special software is needed, [Organization] [REDACTED]
[REDACTED] and [REDACTED] will notify their [REDACTED]. In consultation with the IT Department, a determination on the purchase and installation will be made.

– Users are responsible for ensuring they are working on a secured site as defined by HTTPS when performing online transactions.

– Users will connect only [REDACTED] and the [REDACTED]
[REDACTED]

– Users are not allowed to [REDACTED] using [REDACTED]
[REDACTED] provided and managed by [Organization] or [REDACTED]
[REDACTED] or [REDACTED]

– Users are not allowed to connect devices or configurations that could interfere with the proper functioning [REDACTED].

– All computers, computer system components, software licenses and computer files accessed through the wireless network must be kept secure [REDACTED]

– The wireless access and passwords used to connect to the [Organization] system belong to [Organization] and remain company property.

- **Anti-Malware**

– Anti-malware security software [REDACTED] to the [Organization] system and network, including the Cloud service.

– Users are responsible for keeping their anti-malware software activated and updated to the latest approved version [REDACTED], the detection of malicious programs, and the improvement of malware detection.

– Anti-malware protection should cover all devices which have access to the [Organization] [REDACTED]

- **Monitoring**

– [Organization] reserves the [REDACTED] and the usage of all [Organization]-[REDACTED] to the [Organization] [REDACTED], as well as any [REDACTED] when used to conduct [Organization]-related business.

– Any employee found to have violated this policy may be subject to disciplinary action up to termination of employment.

PROCEDURES

There are no procedures related to this policy.

Policy Title:	PASSWORD POLICY	Policy #:	xxx
Issued by:	Business Services	Original Date:	xxx
ELT Approval:	[Approver's Name] [Approver's Position]	Revised Date:	

PURPOSE

This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

POLICY STATEMENT

- Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of [Organization], Inc. ([Organization]'s entire organization network. As such, all [Organization] employees, volunteers, contractors and vendors with access to [Organization] systems are [REDACTED]
- The scope of this policy includes all [Organization] [REDACTED] with access to [Organization] [REDACTED] who have or are responsible for an account (or any form of access that supports or requires a password) [REDACTED] [Organization] facility, has access to the [Organization] network or stores any non-public [Organization] information.
- **General**
 - Passwords are confidential. A [REDACTED] may not ask anyone to divulge their password.
 - All user-level passwords (e.g., email, web, desktop computer, etc.) [REDACTED] every 45 days.
 - Passwords may not be inserted into [REDACTED] or [REDACTED]
 - All user-level and system-level passwords must conform [REDACTED]
 - Computer stations will automatically lock via the screen saver after 15 minutes [REDACTED]. The password will need to be entered [REDACTED]

Policy #: xxx

Original Date: xxx

Revised Date:

This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

- Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of [Organization], Inc. ([Organization]'s) entire organization network. As such, all [Organization] employees, volunteers, contractors and vendors with access to [Organization] systems are [REDACTED]
- The scope of this policy includes all [Organization] [REDACTED] [REDACTED] with access to [Organization] [REDACTED] who have or are responsible for an account (or any form of access that supports or requires a password) [REDACTED] [Organization] facility, has access to the [Organization] network or stores any non-public [Organization] information.

- Passwords are confidential. A [REDACTED] may not ask anyone to divulge their password.
- All user-level passwords (e.g., email, web, desktop computer, etc.) [REDACTED] every 45 days.
- Passwords may not be inserted into [REDACTED] or [REDACTED]
- All user-level and system-level passwords must conform [REDACTED]
- Computer stations will automatically lock via the screen saver after 15 minutes [REDACTED]. The password will need to be entered [REDACTED]

- A user account will lock after several unsuccessful attempts. If the account is locked, it will [REDACTED]; or [REDACTED] [Organization] [REDACTED].
- Password history of the last two passwords: This means the last two (2) passwords created [REDACTED]

- **Guidelines for General Password Construction**

- Strong, complex passwords are required to protect the user accounts against breaches caused by weak, easily guessed passwords. Passwords are required to contain:

- [REDACTED]
- [REDACTED]

- **Multifactor Authentication**

- Multifactor authentication is the premise of using a combination of authentication factors, [REDACTED], [REDACTED], and [REDACTED], to confirm the user's identity when logging in to their respective accounts.
- In conjunction with your password, users [REDACTED], such as biometrics, and/or hardware confirmation.

[REDACTED] All users are responsible for keeping their login and user authentication information from being compromised, including ensuring protection [REDACTED]

- All User password protection must be [REDACTED] at [Organization] to protect against increasingly advanced password authentication strategies. This refers to [REDACTED] required to protect access to systems which is in line with the Data Protection Laws and Regulations compliance standards.

- [Organization] Users will be granted access to the network and applications based on [REDACTED]. Access to specific information on [Organization] systems and network infrastructure, request, review and approval of software differs [REDACTED]

- Users must ensure adequate security protection of sensitive information and other assets based on the risk and the requirements of applicable policies. ([REDACTED]).

- All SSO and MFA access must be [REDACTED] before they are reassigned to another person.
- Compliance with relevant SSO and MFA set-ups [REDACTED] so that the appropriate [REDACTED] can be made to the access control systems and system authentication.

- **Password Protection**

- Password Protection Standards: The same password for [Organization] accounts may not be used for other non-[Organization] access ([redacted]). Where possible, do not use the same password for various [Organization] access needs. For example, select one password for the student management system and a separate password for IT systems.
- [Organization] [redacted]; all passwords are to be treated as sensitive, confidential [Organization] information.
- Other Password Protection Considerations
 - If someone demands a password, [redacted]
 - The "[redacted]" feature of applications should not be used.
 - Do not store passwords in a file on ANY computer system ([redacted])
 - If an account or password is suspected to have been compromised, [redacted]
 - Important Reminder – The password on [Organization] cellular phones will need to be changed [redacted] when the computer password is changed. Also, other programs such as Skype for Business [redacted] with the new password.
 - From time to time, [Organization] IT will ask for a password [redacted]. The password should be changed upon the completion of the support task.

● User Data Access

- Internet and email resources provided by [Organization] must be [redacted] and governed by rules of conduct similar to those applicable to the use of other information technology resources.
- Access to or use of Internet and email resources is provided by [Organization] or [redacted], on [redacted].
- Students can only log in and access data [redacted] via the [Organization] student network
- Appropriate log-in and log-out procedures with individualized assigned passwords [redacted]
- Acceptable access to data must be [redacted]
- Workstation physical access is limited to [redacted].
- It is a violation of policy for anyone to [redacted] that has no relevance to his or her role and responsibilities.
- Staff can only login and access data via a [redacted] on the [Organization] [redacted].
- The use of equipment is for the [redacted] [Organization] activities.
- Information residing on the equipment is, without exception, [redacted] [redacted] [Organization].

- The access to and transfer of [redacted] outside of [Organization] activities or access [redacted]
- [Organization] recognizes that program staff may come into contact with [redacted] regarding clients, students, volunteers and contractors.
- All personnel are asked to [redacted] before they get access to the [Organization] [redacted]. [redacted] is a fundamental principle of the organization.
- [Organization] personnel are expected to protect client privacy by [redacted] and by [redacted]. Similarly, accessibility to the electronic version of the client file in the database is to be limited [redacted].
- When at work, or when [Organization] computing or networking resources are employed, using and/or copying of non–licensed software, or software that is not consistent with the [redacted]
- Knowingly installing, or causing the installation of any computer program, code or hardware onto the [Organization] Computer Systems [redacted]

Any employee found to have violated this policy may be subject to disciplinary action, up to termination.

PROCEDURES

There are no procedures related to this policy.

[ORGANIZATION], INC. PROCEDURE

Title: [ORGANIZATION] Clean Desk Policy

Date: xxx

Related Policy: xxx

STANDARDS/PROCEDURE

- A. [ORGANIZATION] intellectual property or confidential client information [REDACTED] in any form [REDACTED] [ORGANIZATION] employee or other authorized person.
- B. [ORGANIZATION] intellectual property or confidential client information may only be stored [REDACTED] by [Organization], Inc., i.e., [ORGANIZATION] Network Drives, [ORGANIZATION] Pulse SharePoint, [ORGANIZATION]'s Yammer, [ORGANIZATION]'s OneDrive for Business, [Organization] Teams and other [ORGANIZATION] IT Approved Cloud Services, i.e., [Organization] Impacts, UltiPro, Raisers Edge, Financial Edge, Etc.
- C. Information stored on Storage Mechanisms that are owned, operated, maintained, monitored, and managed by [Organization], Inc., [REDACTED] [Organization]. Inc.
- D. All Information traffic that traverses [Organization], Inc's local or remote networks [REDACTED] [ORGANIZATION] Information Services.
[REDACTED] [ORGANIZATION] employees may not provide their login or email password to anyone, [REDACTED]
- F. All devices that are connected to [ORGANIZATION]'s internal networks via remote access technologies [REDACTED]. Failure to adhere to the above statement can result in appropriate disciplinary action.
[REDACTED] Mobile and external storage devices, i.e., Flash Drives, Portable Hard Drives, SD Cards, and the like, containing or accessing the information resources at [ORGANIZATION] [REDACTED] at [ORGANIZATION]. This pertains to [REDACTED] to the network at [ORGANIZATION] and includes only [ORGANIZATION] [REDACTED]
- [REDACTED] Non-[ORGANIZATION] employees may not use [ORGANIZATION] [REDACTED]
- I. Employees are not permitted to connect [REDACTED] to the [ORGANIZATION] internal network.

These devices may only connect to the [Organization] [REDACTED]

- J. OneDrive for Business, assigned to the employee by [Organization] IT is the Supported, Authorized Cloud Storage platform for [Organization], Inc. Each [ORGANIZATION] employee received 1 TB of cloud storage. Other Cloud storage, i.e., Box.net, Drop Box, Google G-Drive, etc., [REDACTED] by [Organization] Information Technology department. Do not save [ORGANIZATION] Information aka [ORGANIZATION] Intellectual Property to non-authorized cloud services.
- K. [Organization] [REDACTED] from using removable storage devices and other data storage and physical interfaces for the [REDACTED].
- [REDACTED] The protection of confidential information stored in computer files or transferred must be in compliance with the [Organization] [REDACTED]
- M. This prohibition on data transfer [REDACTED] as a way of [REDACTED] of data loss, theft, damage or misuse, and the spread of malicious software, viruses or malware.

Any employee found to have violated this policy may be subject to disciplinary action up to termination of employment.

[ORGANIZATION] POLICY

Policy Title:	EMAIL POLICY	Policy #:	xxx
Issued by:	Business Services	Original Date:	xxx
ELT Approval:	[Approver's Name] [Approver's Position]	Revised Date:	

PURPOSE

This policy defines the email procedures added to [Organization] Phishing and Work-Life Statements.

POLICY STATEMENT

- All employees, volunteers, contractors and vendors with access to [Organization] systems are (collectively referred to as 'Users') [REDACTED]
- Business or personal contact with individuals initiated via the Internet should be treated with caution and [REDACTED]
- Staff and team members should not [REDACTED] for any purpose which would [REDACTED]
- All use of the [Organization] Internet and email resources for commercial purposes [REDACTED]
- All the staff are [REDACTED] for anything written or presented over email.
- Employees can be disciplined for commentary, content, or images that are fraudulent, defamatory, proprietary, harassing, [REDACTED]
- Employees must:
 - not reveal any information that compromises [Organization] policy or public positions. This means sharing anything that is proprietary and/or confidential to [Organization] [REDACTED]
 - refrain from posting information that could reflect negatively on [Organization] or [REDACTED]
 - show proper respect for the partners and communities that we work with;
 - respect the law, including those laws governing defamation, discrimination, harassment, and copyright and fair use; [REDACTED], partnerships, foundations (or any affiliates') confidential or other proprietary

information, including programs and services, research, information about trademarks, organization strategy, processes, techniques or other technical data or information.

- **IT and Cyber Security Training**

- All contracted persons [redacted] [Organization] IT/Cyber Policies, operating standards and procedures. This applies to all [Organization] contractors and vendors with access to [Organization] systems, [redacted], and [Organization] contracted personnel who are authorized to use [Organization] owned equipment or facilities (collectively referred to as 'Users').
- Contractor employees companies will need [redacted] if that they have an IT and Cyber Security training program, and that the contractor has completed it.
- The intent of the training is to provide a [redacted] the use of [Organization] Computer Systems, equipment and infrastructure. This includes the use of equipment, local and wide area networks, the Internet, computer applications, and components such as scanners, photocopiers, printers etc.
- The training should cover CIPA and Compliant Internet Security and Safety, Technology Equipment Security and Safety, Portable Communication Devices Security and Safety, Computer Software Usage, Data Backup and Management, Confidentiality, Privacy, Intellectual Property, and Social Media.

[redacted] Acceptable IT/Cyber training is considered that which conforms to the mission and purpose of [Organization] [redacted]

- Fully trained contracted personnel [redacted], and verify that the use of information technology resources efficiently and productively contain a clause that claims confidentiality over the contents of any communication.
- All Users are required to [redacted] in accordance with this IT/Cyber Policy.
- It is the responsibility of all team members [redacted] with the most recent version of this policy.
- [Organization] Managers will make sure all users are notified when revisions occur, and it is their responsibility to read and to adhere to the revised guidelines.

PROCEDURES

There are no procedures related to this policy.

[ORGANIZATION] POLICY

Policy Title:	PHYSICAL POLICY	Policy #:	xxx
Issued by:	Business Services	Original Date:	xxx
ELT Approval:	[Approver's Name] [Approver's Position]	Revised Date:	

PURPOSE

This policy defines the physical procedures to access the [Organization] ([Organization]) premises.

POLICY STATEMENT

- All visitors must enter via the [REDACTED]
- All visitors must be registered with the front desk using the [REDACTED]. They will be required to display the badge for the duration of the visit, and check out when leaving.
- Visitors are expected to [REDACTED] while on premises, including making their presence known and not exploiting or otherwise taking advantage of their access to the Center.
- Team members who have reason to believe that suspicious individuals or suspicious activities are occurring on premises are encouraged to bring their concerns to the [REDACTED]
- All employees will be [REDACTED] access the [Organization] Center. They must always [REDACTED] when entering the building. The badges are restricted to the use of each employee only, [REDACTED]. Each employee is responsible for keeping their badges in working order, [REDACTED]
- **Surveillance and Monitoring**
 - [Organization] monitors all activity of all employees and visitors on its premises via CCTV. [REDACTED], including employee entrance, visitor entrance, public areas, hallways, stairways, meeting rooms, offices, the perimeter of the building and the designated parking area.
- The installation of the video surveillance system and the retention of the records of surveillance is done in accordance with the legal and legitimate protection of the Center. The surveillance and monitoring is used in a [REDACTED]

PROCEDURES

There are no procedures related to this policy.

Copyright – The Write Direction Inc.