

Information & Security Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.7

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	15/6/2017	P.Sahoo	S K Patel	P Mohanty	
1.1	14/6/2018	P.Sahoo	A Bhatia	P Mohanty	Reviewed
1.2	14/6/2019	P.Sahoo	Ranjeet Singh	Amit Sobti	Reviewed
1.3	26/6/2020	P.Sahoo	Ranjeet Singh	Amit Sobti	Reviewed
1.4	28/6/2021	P.Sahoo	Ranjeet Singh	Amit Sobti	Reviewed
1.5	28/6/2022	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.6	28/6/2023	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.7	28/7/2024	P.Sahoo	Shankar VRG	Amit Sobti	Reviewed

1.0 Purpose

This policy establishes specific requirements for the proper classification and handling of sensitive and confidential information in order to ensure that the Company maintains strict confidentiality in compliance with applicable requirements and regulations.

Additionally, the Policy for Safeguarding Sensitive and Confidential Information is intended to help Company share holder determine what information can be disclosed to non-employees and how, as well as the relative sensitivity of information that should not be disclosed within or outside of Company without proper authorization.

2.0 Scope

This policy pertains to the security and privacy of all non-public information including, employee information, constituent information and general Company information whether it is in hard copy or electronic form.

Accordingly, documents that include sensitive and confidential information such as social security numbers, dates of birth, employee education records, medical information, benefits information, compensation, loans, or financial aid data, employee evaluations need to be secured during printing, transmission (including by fax), copying, storage and disposal.

The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All Company employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to secure personally identifiable information and BPO CONVERGENCE Company Confidential information. Questions about the proper classification of a specific piece of information should be addressed to your Dean or direct supervisor.

3.0 Sensitivity Classification of Information Assets

All BPO Convergence Company information that is stored, processed or transmitted by any means shall be classified into one of four levels of sensitivity: Public, Internal, Confidential and Private. The sensitivity classification identifies information in terms of what it is and how access, processing, communications and storage must be controlled. If more than one sensitivity level could apply to the information the highest level (most restrictive) will be selected.

Note: A sensitivity classification shall attach to and follow the information to which it applies until such time that the classification is changed by the Data Owner/Custodian (see Glossary)

1. **Public** – (Least restrictive) Information that has been declared public knowledge by Company or by someone else who is duly authorized by the Company to do so, and thus may be freely distributed. The disclosure, unauthorized access, or unauthorized use of Public information would not adversely impact the Company, its employee or the public. Accordingly,

Examples of **Public** information include:

- Board of Director Details
- Employee bios
- Company catalogs
- Press releases and marketing materials

2. **Internal** – Information that is available to business units and used for official purposes but would not be released to the public unless requested pursuant to and authorized by applicable law. The disclosure, unauthorized access, or unauthorized use of internal information would have a limited adverse impact on the Company, the State, and/or the public.

Examples of **Internal** information include:

- Financial accounting information
- Department project data such as construction plans that do not impact Company security
- Unit budgets
- Purchase Orders
- Company policies and policy manuals
- Company memos and email, non-public reports, budgets, plans, and financial information
- Non-public contracts

- Employee ID numbers without any other identifying information

3. **Confidential** – Information of a sensitive nature that is available only to designated personnel. The disclosure, unauthorized access, or unauthorized use of confidential information would have a significant adverse impact on the Company. Confidential information is information that is not available to the public under all applicable laws,

Examples of **Confidential** information include:

- Medical examiner and other medical records
- Passport and visa numbers
- Criminal investigations, Campus Police records and evidentiary materials
- Advisory, consultative or deliberative material
- Victims records
- Trade secrets and proprietary commercial or financial information obtained from any source
- Documents subject to attorney client privilege
- Administrative or technical information regarding computer hardware, software and networks which would jeopardize computer security
- Emergency or security information for any building that would jeopardize security of the building or persons therein
- Security measures and surveillance techniques
- Information that would give an advantage to competitors or bidders

- Sexual harassment complaints and investigations
- Grievances filed
- Collective bargaining negotiations
- Communications with insurance carriers or risk management officers
- Information required to be kept confidential by court order
- Social security numbers, credit card numbers, unlisted telephone numbers, and driver's license numbers
- Certain pedagogical, scholarly and/or academic research records
- Test questions, scoring and other examination data
- Employee records, grievance or disciplinary proceedings
- Personnel and pension records

4. **Private** – (most restrictive) All personally identifiable information (PII) pertaining to individuals that is protected by Law. The disclosure, unauthorized access, or unauthorized use of Private information would have a significant adverse effect on the Company,

Examples of **Private** information include:

- Bank Account numbers
- Personal financial information, including checking or investment account numbers

- Driver's License numbers
- Health Insurance Policy ID Numbers
- Unlisted telephone numbers
- Employee directory information that an employee has requested not to be disclosed
- employee ID numbers combined with full names and/or birth dates

4.0 Handling and Distribution of Information Assets

Many employees generate or are exposed to sensitive Company information and personally identifiable information (PII) in the course of their jobs and use it to perform important functions. It is vitally important that all employees handle such information properly. Often, such information contains personally identifiable data that places individuals at risk of identity theft. It may also contain proprietary information, research findings or other intellectual property.

Access to non-public, sensitive information is restricted to those who have a need to know as defined by job duties and access is subject to Company authorized approval. Anyone who receives non-public sensitive information has a responsibility to maintain and safeguard that information and to use it with consideration of that regard for others. Circumventing or attempting to circumvent restrictions on the use and dissemination of internal, confidential, or private information is considered a serious offense and may be subject to discipline. If such information is received in error, the recipient has an obligation to alert the sender that they have received this information in error, and to properly delete and or destroy the received copy of the information.

The release or exchange of individual or Company information may only be made by Company employees in accordance with the guidelines outlined below.

In general, BPO CONVERGENCE Company personnel are expected to use common sense judgment and to handle data categorized as Internal, Confidential, and Private in an appropriate

manner. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should consider it **Private** by default and contact their Vice President, Dean or their designee, or direct supervisor for clarification before taking any action with regard to the information in question.

The guidelines that follow provide details on how to properly handle and/or distribute information with varying degrees of sensitivity, including acceptable electronic transfer and storage methods. Where applicable, disposal guidelines are given as well as the scope of potential penalty for deliberate or inadvertent disclosure.

Please note that these guidelines represent the most common use cases for the handling and distribution of Company data and should be used as a reference only. Information in each category may necessitate more or less stringent measures of protection depending upon the specific circumstances and the nature of the information in question.

Public information

There are no specific restrictions on the distribution or handling of public information, although Company personnel must respect all copyright, trademark and intellectual property rights of any data that they distribute.

Access: Anyone

Distribution within BPO CONVERGENCE Company: No restrictions

Distribution outside of BPO CONVERGENCE Company: No restrictions **Storage:** No restrictions

Disposal/Destruction: Not applicable

Penalty for deliberate or inadvertent disclosure: None

Internal information

Internal information is considered non-public and should be protected from unnecessary exposure or transmission to parties outside of the Company.

Access: BPO CONVERGENCE Company employees, or non-employees with signed non-disclosure agreements, who have a legitimate business or academic need to know.

Distribution within BPO CONVERGENCE Company: Standard interoffice mail, campus email, password-protected web site, or campus file sharing repositories.

Distribution outside of BPO CONVERGENCE Company: encrypted email, password-protected file, password-protected web site to retrieve encrypted file, secure electronic file transmission with file encryption.

Storage: Hardcopy must be stored in a physically secure area (i.e. locked file cabinet) Information may only be stored electronically on Company-owned and maintained computers or on a remote site such as a cloud storage provider that is under contract with the Company for such services.

Regardless of physical storage location, it is recommended that files containing information classified as Internal be stored in an encrypted format. Acceptable forms of encryption are password protected files (i.e. Microsoft Office password protection) or a public/private key algorithm such as PGP or GnuPG.)

Disposal/Destruction: Shred hardcopy; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination of employment, possible civil and/or criminal prosecution.

Confidential information

Confidential information should be protected to prevent unauthorized access or exposure.

Access: BPO CONVERGENCE Company employees whose job functions require them to have and are approved by their supervisor to have access, and Company vendors or consultants who have executed non-disclosure agreements with the Company.

Distribution within BPO CONVERGENCE Company: Delivered direct - signature required, envelopes stamped confidential. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG or be password-protected at the application level (i.e. signed PDF or Word document.) The encrypted/password- protected files can then be sent via email and/or secure electronic file transmission.

Distribution outside of BPO CONVERGENCE Company: Delivered direct; signature required; approved private carriers. Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm such as PGP or GnuPG or be password- protected at the application level (i.e. signed PDF or Word document.) The encrypted/ password-protected files can then be sent via email and/or secure electronic file transmission. Third parties who are handling and/or storing Confidential information must agree to abide by the Company's policies for safeguarding such information.

Storage: Hardcopies must be limited to the minimum number required. Hardcopies must be stored in a secure location at all times. Unless there is a critical business need, no portion of confidential information should be stored locally on employee desktop or laptop computers beyond the Office of Company Counsel. Confidential information may be stored on a Company owned file server, central computing server, or on a remote site such as a cloud storage provider that is under contract with the Company for such services. Regardless of physical storage location, confidential files must be stored in an encrypted format. Acceptable forms of encryption are password protected files (i.e. Microsoft Office password protection), and encrypted hard disk or folder, or a public/ private key algorithm such as PGP or GnuPG.)

Disposal/Destruction: All hardcopy must be cross-cut shredded and disposed of in specially marked disposal bins on BPO CONVERGENCE Company premises; electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

Penalty for deliberate or inadvertent disclosure: Up to and including termination of employment, possible civil and/or criminal prosecution.

Private information

Private information has the highest level of sensitivity and represents the most risk to the Company, the State, and individuals should such information be accessed by or exposed to unauthorized parties. Therefore, Company employees who handle Private information or who use systems that store, transmit, or manipulate Private data are required to maintain the privacy of such information/data at all times.

Access: BPO CONVERGENCE Company employees whose job functions require them to have and are approved by their supervisors to have access, and Company vendors or consultants who have executed non-disclosure agreements with the Company.

Storage: Hardcopies must be limited to the minimum number required. Hardcopies must be stored in a secure location at all times. No Private information may be stored locally on employee desktop or laptop computers, tablet, phone, or on any non-Company device. Instead, Private information.

Must be stored on a Company owned file server, central computing server, or on a remote site such as a cloud storage provider that is under contract with the Company for such services. Regardless of physical storage location, files containing Private information must be stored in an encrypted format. Acceptable forms of encryption include an encrypted hard disk or folder or a public/private key algorithm such as PGP or GnuPG. Password-protecting a file at the application level (ex. PDF or Word document) is not sufficient protection for Private information.

Disposal/Destruction: All hardcopy must be cross-cut shredded and disposed of in specially marked disposal bins on BPO CONVERGENCE Company premises; electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

Penalty for deliberate or inadvertent disclosure: Up to and including termination of employment, possible civil and/or criminal prosecution.

5.0 Guidelines for Protecting Information Stored Electronically

All employees and users of networked computing devices on Montclair's network are responsible for protecting the Company's information because their machines provide potential gateways to private information stored elsewhere on the network. Therefore, whether or not they deal directly with sensitive Company information, employees should take the following steps to reduce risk of unauthorized disclosure of the Company's information:

- Familiarize yourself with all Company security policies and Social Media Policy, and understand their implications for the information for which you are responsible.
- Immediately advise your supervisor of any suspicious activity on your computer or a suspected information system security compromise and report the event to the Company Help Desk for follow-up action.
- Be mindful of how you are sharing or transmitting sensitive information across the network.
- Do not share sensitive information via unencrypted/unsigned email. Unencrypted and unsigned email is not secure; it can be forged, and it does not afford privacy.

- Do not publish sensitive information to unsecured web sites. All sensitive information on web sites must be encrypted and password protected.
- Do not collect Confidential or Private information with web forms that are not secured via https connection with a valid SSL certificate.
- Be certain your machine is always protected from viruses and other malware. Install anti- virus software on your computer and ensure that the software is set to automatically update its virus definitions regularly. (The Information Technology Division distributes the Sophos Antivirus tool at no charge. Please contact the Company Help Desk for more information)
- Take precautions not to send anything by e-mail that you wouldn't want disclosed to unknown parties. Recipients have been known to distribute information to unauthorized recipients or store it on unsecured machines, and viruses have been known to distribute archived e-mail messages to unintended recipients.
- Theft of Montclair State electronic computing equipment must be immediately reported to the Company's Police Department; loss or suspected compromise of Montclair State sensitive data must be immediately reported to the Information Technology Division.
- Ensure that functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.
- Be aware that information stored on laptop computers, tablets, smart phones and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure. Even networks using encryption are vulnerable to intruders.
- Unless there is a legitimate business need, sensitive information that is categorized as Confidential or Private should not be stored on a laptop, desktop, tablet, phone, or other end-user device.
- Employ passwords that comply with the Company's Password Management Policy.

- Secure your passwords, and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe

From unauthorized access.

- Never share your passwords or accounts.
- Restrict file sharing on your computer to mitigate the risk of unintentionally granting access to unknown parties.
- Apply system updates for your desktop systems and department servers' operating systems and their integrated network services (e.g., e-mail and web browsers) in a timely manner.
- Keep local applications updated and patched.
- Encrypt sensitive files. Use IT Security-approved encryption methods only.
- Ensure that remote access (from off campus) connections are done securely using HTTPS, SSH or VPN.

Any employee of the Company found in violation this policy is subject to disciplinary proceedings including suspension of system privileges, termination of employment and/or legal action as may be appropriate and in accordance with the applicable employment handbook, collective bargaining agreement to the individual's relationship to the Company.

6.0 Glossary of Relevant Terms and Definitions

Access Controls

Access Controls are methods of electronically and/or physically protecting files from being accessed by people other than those specifically designated by the owner.

Data Custodian

The **custodians** of data are employees, departments, colleges, research centers, and extension offices responsible for the integrity, confidentiality and availability of the data. It shall be the responsibility of the owner or custodian of the data to classify the data. However, all individuals accessing data are responsible for the protection of the data at the level determined by the owner/custodian of the data. Any data not yet classified by the owner/custodian shall be deemed **Private**.

Data Owner

The entity to which the data belongs. For example, a person owns his/her social security number, date of birth, and address.

Expunge

To reliably and irretrievably erase data from a storage medium such as magnetic disk or tape, or from electronic media such as flash memory. In most cases special software utilities are required to repeatedly overwrite data with random values to make subsequent retrieval of the original data impossible.

Personally Identifiable Information (PII)

The term “PII,” refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that

Is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Secure Electronic File Transmission Methods

Includes Secure FTP (SFTP), Secure Copy (SCP) and Secure Shell (SSH) protocols.

Unencrypted data ("clear text")

Unencrypted data is able to be viewed as-is without the need for a password or software key and is often referred to as clear text.

7.0 SYSTEM ACCESS CONTROL

End-User Passwords

BPO Convergence has an obligation to effectively protect the intellectual property and personal and financial information entrusted to it by Employees, employees, partners and others. Using Password that are difficult to guess is key step toward effectively fulfilling that obligation.

Any password used to access information stored and/or maintained by BPO Convergence must be at least 8 characters long, contain at least one uppercase letter and one number or special character.

Passwords will expire quarterly - every 90 days. When a password expires or a change is required, users should create a new password that is not identical to the last three passwords previously employed.

Passwords stored electronically may not be stored in readable form where unauthorized persons might discover them.

Passwords may not be written down and left in a place where unauthorized persons might discover them.

Passwords may never be shared or revealed to anyone other than the authorized user.

If a password is suspected of being disclosed or known to have been disclosed to anyone other than the authorized user, it should be changed immediately.

Password System Set-Up

All computers permanently or intermittently connected to BPO Convergence local area networks must have password access controls. If the computers contain confidential or protected information, an extended user authentication system approved by the Information Technology department must be used.

Multi-user systems (servers) should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know. Network- connected, single-user systems must employ hardware or software controls approved by Information Technology that prevent unauthorized access.

All vendor-supplied default fixed passwords must be changed before any computer or communications system is used in production. This policy applies to passwords associated with end-user user IDs and passwords associated with privileged user IDs.

Whenever system security has been compromised or if there is a reason to believe that it has been Compromised, the involved system administrator must immediately take measures to ensure that Passwords are properly protected and requiring users to change them prior to next system log on

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must take measures to restore the system to secure operation. This may involve reloading a trusted version of the operating system and all security-related software from trusted storage media or original source-code disks/sites. The involved system then would be rebooted. All changes to user privileges taking effect since the time of suspected system compromise must be reviewed by the system administrator for unauthorized modifications.

Logon and Logoff Process

All users must be positively identified prior to being able to use any BPO Convergence multi-user computer or communications system resources. Positive identification for internal BPO Convergence networks involves a user ID and password, both of which are unique to an individual user, or an extended user authentication system.

Positive identification for all Internet and remote lines involves the use of an approved extended user authentication technique. The combination of a user ID and fixed password does not provide sufficient security for Internet or remote connections to BPO Convergence systems or networks. Modems, wireless access points, routers, switches or other devices attached to network-connected workstations located in BPO Convergence offices are forbidden unless they meet all technical requirements and have a user authentication system approved by the Information Technology department.

The logon process for network-connected BPO Convergence computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters may not be provided until a user has successfully provided both a valid user ID and a valid password.

If there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system should automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is 30 minutes. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room

badge readers, or similar technology or if the suspended session interferes with the ability of an instructor to complete his/her classroom instructional activities.

With the exception of electronic bulletin boards or other systems where all regular users are anonymous, users are prohibited from logging into any BPO Convergence system or network anonymously. If users employ systems facilities that permit them to change the active user ID to gain certain privileges, they must have initially logged on employing a user ID that clearly indicates their identity or affiliation.

8.0 SYSTEM PRIVILEGES

Limiting System Access

The computer and communications system privileges of all users, systems, and independently-operating programs such as agents, must be restricted based on the need to know. This means that privileges must not be extended unless a legitimate academic/business-oriented need for such privileges exists.

Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a system file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Default file permissions granted to limited groups of people who have a genuine need to know are permitted.

Users with personally-owned computers are responsible for administering a screen saver program securing access to their machine's hard disk drive, and setting passwords for all applications and systems software that provide the capability of connecting to BPO Convergence resources.

BPO Convergence computer and communications systems must restrict access to the computers that users can reach over BPO Convergence networks. These restrictions can be implemented through routers, gateways, firewalls, wireless access points, and other network components. These restrictions must be used to, for example, control the ability of a user to log on to a certain computer then move from that computer to another.

Process for Granting System Privileges

Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before a system administrator fulfills these requests. Documents reflecting these requests must be retained for a period of at least one year.

Individuals who are not BPO Convergence employees, Employees, or partners may not be granted a user ID or be given privileges to use BPO Convergence computers or networks unless the written approval of a current employee has been obtained and the employee agrees to full responsibility for all activities carried out by the individual(s) she or he is sponsoring. This can be accomplished using the Sponsored Account Request form.

Privileges granted to users who are not BPO Convergence employees must be granted for periods of 180 days or less. As needed, users who are not BPO Convergence employees must have their privileges reauthorized by the sponsoring department head every 180 days.

Special privileges, such as the default ability to write to the files of other users, must be restricted to those responsible for systems administration or systems security. An exception to this policy may be made if there is a justified business/academic need and permission is acquired through the exception process, using the Exception form. Configuration changes, operating system changes, and related activities that require system privileges must be performed by system administrators.

Third-party vendors must not be given Internet or remote privileges to BPO Convergence computers or networks unless the system administrator determines that they have a legitimate business/academic need. These privileges must be enabled only for the time period required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods.

All users wishing to use BPO Convergence internal networks or multi-user systems that are connected to BPO Convergence internal networks signify their agreement to comply with all applicable policies by their logon to the network.

Process for Revoking System Access

All user IDs should have the associated privileges revoked after a certain period of inactivity not exceeding 90 days.

If a computer or communication system access control subsystem is not functioning properly, it should default to denial of privileges to users. If access control subsystems are malfunctioning, the systems should remain unavailable until such time as the problem has been rectified.

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the IT Infrastructure Services director. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of BPO Convergence policy. Customer/Employee requests that BPO Convergence security mechanisms be compromised must not be satisfied unless the IT Infrastructure Services director approves in advance or BPO Convergence is compelled to comply by law. Short-cuts bypassing systems security measures, pranks, and practical jokes involving the compromise of systems security measures are absolutely prohibited.

The privileges granted to users, based on their role within the organization, should be reevaluated by administration annually. In response to feedback from executives, department managers, the Human Resources department, or the IT Infrastructure Services director, system administrators must promptly revoke all privileges no longer needed by users.

Department heads/Directors must report all significant changes in employee duties or employment status promptly to the Information Technology department or system administrators (for non-IT managed systems) responsible for user IDs associated with the involved persons. For all terminations, the Human Resources department must issue a notice of status change to the Information Technology department and all system administrators who might be responsible for a system on which the involved employee might have a user ID.

ESTABLISHMENT OF ACCESS PATHS

Changes to BPO Convergence internal networks include loading new software, changing network addresses, reconfiguring routers, and adding remote lines. With the exception of emergency

situations, all changes to BPO Convergence computer networks must use the formal change management process and be documented in a work order request. In addition, the Request for Change (RFC) must be approved in advance by the Information Technology Infrastructure Services Director except as delegated Emergency changes to networks must be made by persons who are authorized by Information Technology. This process prevents unexpected changes from leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees, but also to vendor personnel.

Employees must not establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, illegal Peer-to-Peer sharing

Other multi-user systems for communicating information without the specific approval of the IT Infrastructure Services director. New types of real-time connections between two or more in- house computer systems must not be established unless such approval is obtained.

Participation in external networks as a provider of services that external parties rely on is prohibited unless BPO Convergence legal counsel has identified the legal risks involved and the Chief Information Officer has expressly accepted these and other risks associated with the proposal.

Acquisition of technology services or relying on an external party for network or computing services is prohibited unless BPO Convergence legal counsel has identified the legal risks involved, the Chief Information Officer has expressly accepted these and other risks associated with the proposal, and the service provider meets the security and technology requirements identified by the Information Technology department.

All BPO Convergence computers that connect to an internal or external network must employ password-based access controls or an extended user authentication system. Multi-user systems should employ software that restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a system administrator. Single-user systems should employ access control software approved by the Information Technology department that includes boot control and an automatic screen blanker that is invoked after a certain period of no input activity. Portable computers and home/personally-owned computers that contain BPO Convergence information are also covered by this policy, as are network devices such as firewalls, gateways, routers, and bridges.

Remote maintenance ports for BPO Convergence computer and communication systems must be disabled until the time they are needed by the vendor. These ports must be disabled immediately after use.

Portable devices (smartphones, tablet computers, etc.) using Wi-Fi or commercial data networks should not be used for data transmissions containing confidential personal information unless the connection is encrypted. Such links may be used for electronic communications as long as users understand that confidential personal information must not be transmitted using this technology.

COMPUTER VIRUSES, WORMS, AND TROJAN HORSES

Users must keep approved and current virus-screening software enabled on their computers. This software must be used to scan all software coming from third parties or other BPO Convergence departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for damage occurring because of viruses on computer systems under their control. As soon as a virus is detected, the involved user must immediately call the Information Technology department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

All personal computer software should be copied prior to its initial usage, and such copies must be stored in a safe place. These master copies can be used for recovery from computer virus infections, hard disk crashes, and other computer problems.

BPO Convergence computers and networks must not run software that comes from sources other than business/academic partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a testing regimen approved by the IT Infrastructure Services director.

DATA SECURITY

BPO convergence all Computers & Laptops are prevented to access USB & Data Card to secure the data of the organization. BPO convergence employee will not be able to share their data using USB storage devices. If someone plugged their USB storage devices on BPO convergence any systems that time they will receive an error "USB Access was blocked".

DATA AND PROGRAM BACKUP

Personal computer users are responsible for backing up the information stored on their local machines. For multi-user computer (servers) and communication systems, a system administrator is responsible for making periodic backups.

To ensure that valuable or critical data is backed up, it must be stored on network servers managed by the Information Technology department or a trusted partner.

BPO Convergence requires the use of industry-standard media, techniques, and timelines in executing all backups. For multi-user computer systems, whenever systems software permits backups must be performed without end-user involvement, over an internal network and during the off hours.

Storage of backup media is the responsibility of the office computer user or multi-user computer system administrator involved in the backup process. Media should be stored in fireproof safes, at a separate location at least several city blocks away from the system being backed up.

Information listed on the Information Retention Schedule maintained by the Business Office, must be retained for the period specified. Other information must be properly disposed of when no longer needed, which is generally within two years.

Department managers/Directors are responsible for preparing, testing and periodically updating department contingency plans to restore service for all non-IT managed production applications and systems. The Information Technology department is responsible for preparing, testing and periodically updating network service contingency plans.

All Confidential information stored on backup media should be encrypted using approved encrypting methods.

LOGS AND OTHER SYSTEMS SECURITY TOOLS

Every multi-user computer or communications system must include sufficient automated tools to assist the system administrator in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

Whenever cost justifiable, automated tools for handling common security problems must be used on BPO Convergence computers and networks. For example, software that automatically checks personal computer software licenses through a local area network should be used on a regular basis.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical BPO Convergence information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging system configurations.

9.0 RECORD RETENTION AND DESTRUCTION POLICY

- 1) Purpose The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by Bpo Convergence or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of Bpo Convergence in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.
- 2) Policy This Policy represents the Bpo Convergence's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.
- 3) Bpo Convergence has a purging policy as per the contractual requirement of client.

4) ELECTRONIC DOCUMENTS

1. Electronic Mail: Not all email needs to be retained, depending on the subject matter. • All e-mail—from internal or external sources—is to be deleted after 12 months.

2. Staff will strive to keep all but an insignificant minority of their e-mail related to business issues. • Bpo convergence will archive e-mail for six months after the staff has deleted it, after which time the e- mail will be permanently deleted.
3. All Bpo Convergence business-related email should be downloaded to a service center or user directory on the server.
4. Staff will not store or transfer Bpo Convergence related e-mail on non-work-related computers except as necessary or appropriate for {Insert Name of Organization} purposes.
5. Staff will take care not to send confidential/proprietary Bpo Convergence information to outside sources.
6. Staff with more than 500MB in their e-mail account will be unable to send or receive messages until the size of their account is reduced. Staff will be notified by {IT Department} as their account size approaches 500 MB.
7. Any e-mail staff deems vital to the performance of their job s should be copied to the staff's H: drive folder, and printed and stored in the employee's workspace.

Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the Subject matter.

- PDF documents – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.
- Text/formatted files - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace.

10.0 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Under state, regulatory, and contractual requirements, Bpo Convergence is responsible for developing and implementing a comprehensive information security program. The purpose of this document is to clearly define roles and responsibilities that are essential to the implementation and continuation of the Bpo Convergence's Information Security Plan (ISP).

Definitions

- **Information System**—Any electronic system that stores, processes, or transmits information.
- **Information Assets**—Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the Organization.
- **Principle of Least Privilege**—Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.
- **Principle of Separation of Duties**—Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Information Security Board of Review

The Information Security Board of Review (ISBR) is an appointed administrative authority whose role is to provide oversight and direction regarding information systems security and privacy assurance. In collaboration with the Chief Information Officer (CIO), the ISBR's specific oversight responsibilities include the following:

- Oversee the development, implementation, and maintenance of a wide strategic information systems security plan.
- Oversee the development, implementation, and enforcement of Bpo Convergence information systems security policy and related recommended guidelines, operating procedures, and technical standards.
- Oversee the process of handling requested policy exceptions
- Advise the Bpo Convergence administration on related risk issues and recommend appropriate actions in support of the University's larger risk management programs.

Security and Information Compliance Officers

The Security and Information Compliance Officers oversee the development and implementation of the Bpo Convergence's ISP. Specific responsibilities include:

- Ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with federal and state laws.
- Ensure appropriate risk mitigation and control processes for security incidents as required.
- Document and disseminate information security policies, procedures, and guidelines
- Coordinate the development and implementation of a Bpo Convergence -wide information security training and awareness program
- Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of information assets.

Data Owner

A Data Owner is an individual or group or people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, company, or administrative unit of the Organization

The role of the data custodians is to provide direct authority and control over the management and use of specific information. These individuals might be Sites Heads, department heads, managers, supervisors, or designated staff. Responsibilities of a Data Owner include the following:

Ensure compliance with Bpo Convergence policies and all regulatory requirements

Data Owners need to understand whether or not any University policies govern their information assets. Data Owners are responsible for having an understanding of legal and contractual obligations surrounding information assets within their functional areas.

Assign an appropriate classification to information assets

All information assets are to be classified based upon its level of sensitivity, value and criticality to the Organization. Bpo Convergence has adopted three primary classifications: Confidential, Internal/Private, and Public. Please see the Data Classification and Protection Standard for further reference.

Determine appropriate criteria for obtaining access to sensitive information assets

A Data Owner is accountable for who has access to information assets within their functional areas. This does not imply that a Data Owner is responsible for day-to-day provisioning of access. Provisioning access is the responsibility of a Data Custodian.

A Data Owner may decide to review and authorize each access request individually or may define a set of rules that determine who is eligible for access based on business function, support role, etc. Access must be granted based on the principles of least privilege as well as separation of duties.

Approve standards and procedures related to management of information assets

While it is the responsibility of the Data Custodian to develop and implement operational procedures, it is the Data Owner's responsibility to review and approve these standards and procedures. A Data Owner should consider the classification of the data and associated risk tolerance when reviewing and approving these standards and procedures. For example, high risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process.

Understand how information assets are stored, processed, and transmitted

Understanding and documenting how information assets are being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner.

One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Owner.

Implement appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of information assets

Information Technology has published guidance on implementing reasonable and appropriate security controls for the three classifications of data: Confidential, Internal/Private, and Public. Contractual obligations, regulatory requirements and industry standards also play an important role in implementing appropriate safeguards.

Data Custodians should work with Data Owners to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Owner.

Document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of information assets

Documenting administrative and operational procedures goes hand in hand with understanding how data is stored, processed and transmitted. Data Custodians should document as many repeatable processes as possible. This will help ensure that information assets are handled in a consistent manner and will also help ensure that safeguards are being effectively leveraged.

Provision and de-provision access as authorized by the Data Owner

Data Custodians are responsible for provisioning and de-provisioning access based on criteria established by the appropriate Data Owner. As specified above, standard procedures for provisioning and de-provisioning access should be documented and made available to the appropriate Data Owner.

Understand and report security risks and how they impact the confidentiality, integrity and availability of information assets

Data Custodians need to have a thorough understanding of security risks impacting their information assets. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching vulnerability's in a system or application are both examples of security risks.

Security risks need to be documented and reviewed with the appropriate Data Owner so that he or she can determine whether greater resources need to be devoted to mitigating these risks. Information Technology Services can assist Data Custodians with gaining a better understanding of their security risks.

Data Users

All users have a critical role in the effort to protect and maintain Organization information systems and data. For the purpose of information security, a Data User is any employee, contractor or third-party provider of the Organization who is authorized to access Organization Information Systems and/or information assets. Responsibilities of data users include the following:

Adhere to policies, guidelines and procedures pertaining to the protection of information assets

Information Technology publishes various policies, procedures, and guidelines related to the protection of information assets and systems.

Users are also required to follow all specific policies, guidelines, and procedures established by departments, Organization or business units with which they are associated and that have provided them with access privileges.

Report actual or suspected security and/or policy violations or breaches to IT

During the course of day-to-day operations, users may come across a situation where they feel the security of information assets might be at risk. For example, a user comes across sensitive information on a website that he or she feels shouldn't be accessible. If this happens, it is the users responsibly to report the situation.