

# ***COPIES-F.Y.I., INC.***

---

**Policies and Procedures**

**Data Security Policy**

---

## Preamble

Most of Copies FYI, Incorporated financial, administrative, research, and clinical systems are accessible through the campus network. As such, they are vulnerable to security breaches that may compromise confidential information and expose our company to losses and other risks. At Copies FYI, Inc., security is critical to the physical network, computer operating systems, and application programs and each area offers its own set of security issues and risks.

***Confidentiality and privacy, access, accountability, authentication, availability, and Information Technology system and network maintenance*** are components of a comprehensive security plan. This plan identifies key concerns and issues faced by our company at the application, host, and network level, and strives for a balance between our company's desire to promote and enhance the free exchange of ideas and its need for security of critical information and systems.

This document will:

1. Identify the elements of a good security policy;
2. Explain the need for Information Technology security;
3. Specify the various categories of Information Technology security;
4. Indicate the Information Technology Security responsibilities and roles; and
5. Identify appropriate levels of security through standards and guidelines.

This document establishes an overarching security policy and direction for Copies FYI, Inc. Individual clinics, doctors and attorney's and their firms are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.

The elements of a good security policy include:

Confidentiality and Privacy  
Access  
Accountability  
Authentication  
Availability  
Information technology system and network maintenance policy

***Confidentiality*** refers to our company's needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.

***Access*** defines rights, privileges, and mechanisms to protect assets from access or loss.

***Accountability*** defines the responsibilities of users, operations staff, and management.

***Authentication*** establishes password and authentication policy.

***Availability*** establishes hours of resource availability, redundancy and recovery, and maintenance downtime periods.

***Information technology system and network maintenance*** describes how both internal and external maintenance people are allowed to handle and access technology.

Our company and all members of our company are obligated to respect and to protect ***confidential*** data. Medical records, certain employment-related records, attorney-client communications, and certain research and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including clinic and other personnel records, and records relating to our company's business and finances are, as a matter of company policy, treated as confidential.

Systems (hardware and software) designed primarily to store confidential records (such as the Financial Information System and all medical records systems) require enhanced security protections and are controlled (***strategic***) systems to which ***access*** is closely monitored. Networks provide connection to records, information, and other networks and also require security protections. The use of Copies FYI Information Technology assets in other than a manner and for the purpose of which they were intended represents a misallocation of resources and, possibly, a violation of law. Guidelines for appropriate use of computer facilities and services at Copies FYI, Inc can be found at <http://www.copiesfyi.com>.

This policy applies to the following categories of security:

- ***Computer system and applications security***: Central processing unit, peripherals, operating system and data.
- ***Physical security***: The premises occupied by the Copies FYI, Inc. personnel and equipment; which has a security system installed.
- ***Operational security***: Environment control, power equipment, operational activities.
- ***Procedural security***: Established and documented security processes for information technology staff, vendors, management, and individual users.
- ***Network security***: Communications equipment, personnel, transmission paths, and adjacent areas.

***Responsibility for guaranteeing appropriate security for data, systems, and networks is assigned to Copies FYI, Inc management directors, and department heads.*** In many cases, responsibility for designing, implementing, and maintaining security protections will be delegated to information technology staff, but the director, or department head will retain responsibility for ensuring compliance with this policy. In addition to management and information technology staff, the ***individual user is responsible for the information technology equipment and resources under his or her control.***

Copies FYI, Inc., is responsible for:

6. Tracking technology and regulatory changes that may indicate or require a change or addition to the current policy;

7. Advising affected management and staff of said changes;
8. Establishing procedures that support the implementation and maintenance of the security policy;
9. Assisting departments and clinics within Copies FYI, Inc to develop, implement and maintain their own security policies that support and facilitate our company's enterprise policy; and
10. Establishing and maintaining a repository for Copies FYI, Inc.'s collected security documents.

## Confidentiality and Privacy

Our company and all members of our company are obligated to respect and, in many cases, to protect confidential data. There are, however, technical and legal limitations on our ability to protect confidentiality. For legal purposes, electronic communications are no different than paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and more likely to be seen in the course of routine maintenance of computer systems.

Certain areas of our company permit incidental personal use of computer resources. Our company does not monitor the content of personal web pages, e-mail or other on-line communications. However, our company must reserve the right to examine computer records or monitor activities of individual computer users (a) to protect the integrity or security of the computing resources or protect our company from liability, (b) to investigate unusual or excessive activity, (c) to investigate apparent violations of law or Copies FYI policy, and (d) as otherwise required by law or exigent circumstances. In limited circumstances, our company may be legally compelled to disclose information relating to business or personal use of the computer network to governmental authorities or, in the context of litigation, to other third parties,

Administrators of Copies FYI, department or division networks should notify computer users if incidental personal use is not permitted and that our company cannot ensure the confidentiality of personal communications.

## Access

No one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes. Our company's Computer Use Policy (<http://www.copiesfyi.com>) requires that members of our company respect the privacy of others and their accounts, not access or intercept files or data of others without permission, and not use another's password or access files under false identity. Violators of any of these rules are subject to discipline consistent with the general disciplinary provisions applicable to ROI Specialists and staff.

Technology assets are to be housed in an appropriately secure physical location. Technology assets include servers, personal computers that house systems with controlled access (laptops are a category of special consideration), ports (active ports in public areas), sniffing devices (PC's set up to do this for diagnosis should be secure), modems and network components (cabling, electronics, etc.).

Passwords help protect against misuse by seeking to restrict use of Copies FYI systems and networks to authorized users. Authorized users (specific individual) are assigned a unique strong password that is to be protected by that individual and not shared with others, is difficult to crack, is changed on a regular basis, and is deleted when no longer authorized.  
(<http://www.copiesfyi.com>)

The management for each area will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion. Such controls may include some combination of the following: setting up base-line traffic monitoring and comparing with network logs for variances; implementing system control mechanisms to detect unexpected data conditions; monitoring successful and unsuccessful access to data; and, conducting port scans to ensure that only authorized users are connected to the network.

Each Copies FYI controlled information system must have an Access Policy that defines access rights and privileges and protects assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users, operations staff and management. The Access Policy will provide guidelines for external connections, for data communications, for connecting devices to a network, and for adding new software to systems. As part of the policy, the responsibility and accountability for its implementation must be established.

Additionally, as users are granted access to controlled Copies FYI systems, they will receive written statements (specific to the individual application and authored by the security administrator for that application) outlining the user's responsibility regarding the appropriate use of the system and data and emphasizing the consequences of improper use. This statement is to be read and signed by each user.

## Accountability

Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be 'loaned.' Individual users will be held responsible for any security violations associated with their usernames.

Operations staff is responsible for reviewing the audit logs and identifying potential security violations. The operations staff is responsible for establishing the security and access control mechanisms (such as usernames, passwords, logging, etc.) and may be held accountable for any security breaches that arise from improper configuration of these mechanisms.

Each user permitted to access a controlled system is to be made aware of the access policy for that system. Management will provide this information to the employee when first granting access and make the employee aware of the auditing capability in place to verify compliance.

All controlled systems must maintain audit logs to track usage information to a level appropriate for that system. All user sessions and all failed connection attempts must be logged. For user sessions, the following will be recorded: user, source IP, session start time/date, and session end time/date. For failed connection attempts, the number of attempts must also be recorded. Management has the discretion to determine whether additional logging is necessary.

Audit logging may also apply to networks. Logging of network traffic flow and access is a standard practice. If inappropriate use of the network is suspected, and management so requests, Network Technology Services may authorize specific traffic logging on portions of the campus network.

If the operations staff believes a security incident has occurred, they will immediately notify their management. Management will assess the potential implications of the incident, notify Network

Technology Services, and take any remedial and necessary action. All audit logs will be immediately duplicated and moved to secure media for further analysis.

Before adding new software to Copies FYI computers and networks, system defaults should be carefully reviewed for potential security holes and passwords shipped with the software should be changed. Downloading software, particularly software that is not job-related or endorsed by the administration, may introduce security risks and should be controlled.

## Authentication

Authentication and data encryption or point-to-point communication will be implemented for all systems that send or receive sensitive data or when it is critical that both parties know with whom they are communicating. The decision of whether to encrypt data should be made by the professional system administrator responsible for the particular application being distributed, with the knowledge of the appropriate director, or department head.

## Availability

Mission critical systems are expected to be available at all times during applicable business hours. Each critical system must have a published availability statement which details redundancy and recovery procedures, and specifies hours of operations and maintenance downtime periods. It must also include contact information for reporting system outages. This statement must be submitted to and approved by Network Technology Services.

Backup of data will be well-documented and tested. Backups of mission critical data must be maintained in secure off site storage to guard against the impact of disasters.

## Information Technology Systems and Network Maintenance

In the course of doing business, Copies FYI, Inc Information Systems management, Network Technology Services, and all departments may contract for all or some system and network local or remote maintenance or support. Representatives of these contracted companies must follow all Copies FYI policies.

Copies FYI, Inc. is expected to establish appropriate guidelines for building, equipment and system access. It is the responsibility of the contracting clinic to inform the contractor of all appropriate policies and, in addition, to provide oversight of the contractor and contractor representatives during the time they have access to Copies FYI resources.

## Reporting Violations

Owners or managers of computer, network, or applications systems, as well as users of these systems, have the responsibility to report any apparent violations of law, Copies FYI policy (<http://www.copiesfyi.com>) to local management and Network Technology Services or Computing and Communications whenever such violations come to their attention.

Owners and managers of department computing, network, and applications systems shall make available to management and users of the systems guidelines for reporting security violations. These guidelines will provide specific guidance on what, when, where, to whom, and within what timeframe the violation should be reported and a copy will be filed with Network Technology Services or Computing and Communications.