

# **Attachment L**

## **Indiana Election Division Statewide Voter Registration System**

### **Security Policy Guideline**

---

# State of Indiana

---

## Enterprise Information Technology Security Policy Guideline

## Table of Contents

|   |           |
|---|-----------|
| <b>Overview</b> .....   | <b>3</b>  |
| <b>Objective</b> .....  | 3         |
| <b>Scope</b> .....  | 3         |
| <b>Executive Summary</b> .....  | 3         |
| <b>Enterprise Policy</b> .....  | 4         |
| <b>Effective Date</b> .....   | 5         |
| <b>Maintenance</b> .....  | 5         |
| <b>Statutory Authority</b> .....  | 5         |
| <b>Guiding Principles</b> .....   | 6         |
| <b>Responsibilities</b> .....   | 6         |
| ITOC is responsible for:.....   | 6         |
| Division of Information Technology (DoIT) is responsible for: .....     | 6         |
| Indiana Telecommunications Network (ITN) is responsible for:.....       | 6         |
| State Board of Accounts is responsible for:.....                        | 7         |
| Indiana Department of State Personnel is responsible for:.....          | 7         |
| All agencies are responsible for:.....                                  | 7         |
| <b>Platform Policies</b> .....  | 7         |
| <b>Servers</b> .....  | 7         |
| <b>Workstation</b> .....  | 9         |
| <b>Network</b> .....  | 9         |
| Wireless Network Connectivity .....                                     | 13        |
| Intrusion Detection.....  | 13        |
| Firewall .....  | 15        |
| Router / Switches .....   | 16        |
| <b>Virus Protection</b> .....   | 18        |
| <b>Protection for the Privacy of Personally Identifiable Data</b> ..... | 18        |
| <b>Protection of Software and Other Copyrighted Material</b> .....      | 19        |
| <b>Information and Data Sharing</b> .....                               | 20        |
| <b>Computer Use Policy</b> .....  | 21        |
| <b>Personnel Security Practices</b> .....                               | 21        |
| <b>Physical Security</b> .....  | 22        |
| <b>Incident Response</b> .....  | 23        |
| <b>Off-site storage and environmental controls</b> .....                | 23        |
| <b>Business Continuity/Disaster Recovery Plan</b> .....                 | 24        |
| <b>Surplus Computer Equipment and Media</b> .....                       | 25        |
| <b>Conclusion</b> .....   | <b>25</b> |
| <b>Appendix A</b> .....   | <b>26</b> |
| <b>Appendix B</b> .....   | <b>28</b> |
| <b>Appendix C</b> .....   | <b>30</b> |

## Overview

### Objective

The purpose of this document is to provide the state agencies with an information technology (IT) security policy, which is required to safeguard data, computing and telecommunications facilities, including hardware, software, and personnel against security breaches. Each agency must be able to demonstrate the ability to comply with this policy.

The principal priorities of information technology (IT) security are:

- To maintain data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data
- To prevent misuse of, damage to, or loss of IT hardware, software, and facilities
- To maintain employee accountability for protection of IT assets
- To prevent unauthorized use or reproduction of copyrighted material

The Information Technology Oversight Commission (ITOC) requires that each state agency provide the following to comply with the Enterprise Information Technology Security Policy:

- Develop, implement, enforce, maintain, and audit IT security plans
- Develop and maintain a security awareness program for training their employees in proper security procedures and standards
- Implement proper security measures needed to protect voice, video and computer data, hardware, software, facilities, personnel and application systems
- All computer application systems which process financial information must maintain adequate control over modification of computer processing capabilities and financial information by technical staff and system users

### Scope

This policy applies to all state agencies that connect to the State of Indiana campus area network (CAN) through a local area network (LAN), metropolitan area network (MAN) or wide area network (WAN). Additionally, agencies that use the extranet only are subject to the section titled "Allowed Inbound Network Traffic to the Extranet."

### Executive Summary

In developing plans to protect and guard against potential malicious attacks and maintain integrity on the state resources, this document, provides minimum requirements for security policies related to:

- Servers
- Workstations
- Network

- Virus Protection
- Protection of Copyrighted Material
- Computer Use
- Personnel Security
- Physical Security
- Off-site Storage
- Surplus of Computer Equipment and Media

This document defines the roles, policies, and operational requirements for monitoring and ensuring security across the organization's platform infrastructure.

## **Enterprise Policy**

Each agency using data, voice, video telecommunications, or computer services for carrying out its mission must develop an IT security plan. Each agency is responsible and accountable for its own IT security plans. Agencies must document their IT security plans in accordance with standards provided by this policy. The amount of detail included in the security plan, and the security measures, should be commensurate with the size, complexity, fiscal value, and potential business exposure of the installation. Agencies must update their IT security plans at least annually and following any significant change to their business, computing, or telecommunications environment. Agency Heads or where available IT Directors shall review and approve the updated plan and submit to ITOC for review. Each security plan must contain enough information to enable agency management to ensure the agency's ability to protect the integrity, availability, and confidentiality of agency information and to protect IT assets from unauthorized use or modification and from accidental or intentional damage or destruction. Each security plan may contain references to another organization's IT security plan or to an agency's internal policy, standards, or procedures manual. The agency shall, upon request, make referenced material available for review or audit. Agencies must, evaluate, certify, and test their security plans and procedures at least once a year. The testing or validation methodology adopted by an agency will depend on:

- Criticality of agency business functions
- Cost of agency IT (value of data and systems)
- Cost of executing the test plan
- Complexity of information systems and components; and
- Complexity of telecommunications systems and components

By evaluating your security plan on a regular basis, you are provided a current look at your security posture, ensuring any new requirements or changes to your system are adequately protected.

By having your security plan, policy and implementation certified by a third party you will be assured that your network is adequately protected based on the certification criteria.

A “Certification” states that the security requirements provided in 45 C.F.R. Part 142 are being met in order to comply with HIPAA security standards. An outside firm and or a state agency can accomplish third party certification.

Security awareness training for employees is also a required process in the Security Plan. Agencies must make their employees aware of the need for IT security. Agencies shall train their employees to perform the security procedures required of them.

The State Board of Accounts may audit agency IT security plans for compliance with the specified standards. If two or more agencies participate with each other in operating an information service facility, then the agencies must develop a joint IT security plan, which meets their mutual needs. Platform policies must comply with this document. Any non-compliance should be noted in a separate section with a request for exception submitted to ITOC.

### **Effective Date**

All agencies will submit their security plans to be in compliance with this policy no later than June 30, 2003. Agency plans must be executed and in place by June 30, 2004.

### **Maintenance**

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to the standards adopted under this policy. The security domain architecture team is responsible for routine maintenance of the standards. Only major policy shifts require ITOC approval.

### **Statutory Authority**

ITOC has been granted the authority to create, implement and enforce this IT policy as stated in: IC 4-23-16.

As stated in IC 4-23-16-5b “It shall be the responsibility of the commission to coordinate the operations of the various information technology systems within the executive, including the administrative, branch of state government insofar as is possible without infringing upon the prerogatives of the separately elected state officials. The objectives of the commission shall be to develop consistent policy and to promote economical, effective, and integrated information technology services, technology accessibility, operational security, and adherence to the principles of the code of fair information practices for individual privacy.”

The purpose of this iteration of the code is to make aware that separately elected officials are not required to follow this policy. However, it **is** the responsibility of ITOC to develop and provide operational security for the state’s backbone. If all state government entities connected to the backbone does not adopt this policy, there is the potential for increased security vulnerabilities. Appropriate action will be taken to disconnect any state entity whose connectivity is determined to be a threat to the backbone.

## **Guiding Principles**

The responsibility and accountability for protecting the state of Indiana's information technology infrastructure lies with every state employee, contractor, and vendor. This includes the protection of state owned hardware, software, data, and personal information regarding our constituents as well as our employees.

Information technology security is necessary to ensure that no individuals or organizations with malicious intent can effectively harm the infrastructure and thereby prevents us from providing the service and support to the state.

## **Responsibilities**

### **ITOC is responsible for:**

- Development, maintenance, and enforcement of the state of Indiana's Enterprise Security roles, policies, standards, audits, and business process reviews
- Development and publication of the Information Technology Security Architecture

### **Division of Information Technology (DoIT) is responsible for:**

- Development, maintenance, and monitoring of Network Security roles, policies, standards, tools, and procedures
- Design and maintenance of a secure state network on the CAN/MAN by
  - Monitoring network traffic for potential intrusion detection
  - Maintaining most current virus protection engine and signature files on their servers
  - Assisting agencies in the development of their security infrastructure on a billable basis, when requested
  - Controlling the setup and use of network firewalls, routers and switches
  - Assisting agencies in the recognition and reporting of potential security violations
- Development and maintenance of incident response procedures
- Adherence to state wide information security policies and procedures on any devices they manage
- Investigation and reporting of attack incidents on the campus area and metropolitan area networks
- Mainframe and shared servers security
- Determine trusted and un-trusted networks on the state Intranet and Extranet

### **Indiana Telecommunications Network (ITN) is responsible for:**

- Design and maintenance of a secure state WAN by:
  - Maintaining most current virus protection engine and signature files on their servers
  - Controlling the setup and use of network routers and switches
- Development and maintenance of incident response procedures
- Adherence to state wide information security policies and procedures on any devices they manage

- Investigation and reporting of attack incidents on the ITN network
- Define and determine trusted and un-trusted networks on the state Intranet

**State Board of Accounts is responsible for:**

- Auditing of agency security policies and procedures for systems that manage the State's fiscal assets
- Auditing of DoIT and ITN security procedures
- Maintain documentary evidence of compliance to security policies and procedures

**Indiana Department of State Personnel is responsible for:**

- Developing policies that provide sanctions for non-compliance by state personnel to security policy
- Incorporating security training and awareness in state personnel employment orientation program

**All agencies are responsible for:**

- Development, enforcement and maintenance of agency level security plans, policies and procedures, see appendix A for a security plan outline
- Security training and awareness procedures for agency
- Compliance with enterprise level security policies and procedures
- Annual review of each employee's access to computer systems and data to ensure adequate segregation of duties to help prevent errors or fraud
- Assigning an agency security manager responsible for the oversight of agency security needs and requirements, see appendix B for a sample job description

## Platform Policies

### Servers

#### Introduction

Servers include mainframe, mini, and microcomputers that are used to host software, databases, applications, and/or operating systems. Servers are secured through a combination of configuration and user authentication standards and procedures.

#### Policy

Any agency that maintains servers will develop a server security policy that details the installation procedures that provide the required security needed to protect the data and hardware from malicious attacks and continued maintenance required to keep the security current.

DoIT administers all Mainframe security through RACF. The RACF policy can be accessed through the ITOC web site at

[http://www.in.gov/itoc/html\\_site/architecture/poli.html](http://www.in.gov/itoc/html_site/architecture/poli.html) . Agency users of the mainframe must adhere to the RACF policy.

While DoIT is responsible for the policy, agencies that utilize servers maintained by DoIT shall work with DoIT administrators to ensure their data is secured to the appropriate level required by agency standards and based on value of the information.

## **Operational Requirements**

### **User authentication**

The following are configuration and user authentication procedures that should be followed:

- Each user must have a unique user identification code and password
- Passwords must be changed every 30 days
- Passwords must be a minimum of six (6) characters in length
- Passwords must be a combination of alphabetic and numeric characters
- Passwords may not be the same as the user identification code and as the last five (5) passwords used by this user identification code
- Individuals must assign their own passwords. At first logon, the user must be required to change all administrator assigned passwords
- Passwords must be encrypted while stored on the computer
- User identification codes and passwords may not be shared
- Users other than System Administrators and Security Administrators must be prevented from accessing sensitive operating system commands and operating system and computer program files. Use of role based security is highly recommended
- User identification codes must be deactivated and user locked out of system after three unsuccessful attempts to sign on to the computer
- User access rights must be eliminated or revised upon termination of employment or transfers of employee responsibility
- Passwords must be changed as soon as they expire with a limit of three grace logons within ten business days
- Logon Ids' may only be acquired through written request
- Passwords are to be excluded from batch files if at all possible
- All unauthorized access attempts to servers should be fully investigated by the state agency and/or DoIT
- Passwords for hardware and software vendors, used during installation, must be changed or deleted upon completion of the installation

### **Configuration**

- Do not use default setup for NOS installations
- Disable all non-essential services
- Install network Virus protection
- Maintain a clean and safe environment

- Ensure use of a NTFS file system

## Workstation

### **Introduction**

A workstation is a personal computer or terminal assigned for end user access to server and/or network based computing. With workstations being used to access the various networks, Internet, Intranet, and Extranet they provide a good avenue for malicious attacks on the state's networked environment. Therefore, workstations must be protected, and security enabled, to alleviate the potential vulnerability the workstation presents.

### **Policy**

All agencies will ensure all workstations have known vulnerabilities disabled within the setup of the operating systems. Workstations will be maintained on a regular basis to ensure all needed patches and or fixes are installed. Setup will be based on the minimum criteria as outlined in the next section.

### **Operational Requirements**

All workstations will be installed with the following minimum-security functions:

- Workstations operating system will not be installed using default settings
- Workstations are subject to the same level of user authentication as noted above for servers
- The last attempted sign-on for a user identification code must not be displayed when a user signs on the computer
- For inactive terminals, the user must be automatically prevented from accessing the computer after 15 minutes of no activity until the user password is entered
- Passwords should not be displayed at or near the workstation
- Virus protection should be installed and scheduled for automatic updates on a weekly basis
- When leaving a workstation unattended user must logoff to prevent unauthorized access or use the lock computer function

## Network

### **Introduction**

A network is defined as a system of interconnected hardware and software capable of sharing data and resources. This includes workstations, servers, printers, routers, switches and firewalls utilizing coax, fiber, or wireless technology. The state of Indiana has a diverse network including LAN's, CAN's, and WAN's that provides the agencies with the ability to communicate, share data and resources, and publish information for the public. These networks require protection from potential threats.

## **Policy**

DoIT will be responsible for the security of the state's campus area network (CAN) and the metropolitan area network (MAN). ITN is responsible for the security of the wide area network (WAN). DoIT and ITN are jointly responsible for the point of convergence between the CAN and the WAN.

All agencies with their own internal LAN are responsible for the security and protection of their respective data, hardware, and software resources. Each agency will develop a security plan detailing the processes and procedures in the protection and securing of their LAN.

## **Operational Requirements**

### **Network Categorization**

A network can be categorized into three groups according to their security position:

- Trusted - networks where no state security issues exist and whose security is under control of the state
- Un-trusted – networks where potential security issues reside and the security is not under the control of the state
- Partially Trusted – the security of the remote network is not controlled by the state or cannot be guaranteed and potential security issues exist

### **Network Structure**

DoIT will maintain three separate networks for the use by State personnel, contractors, clients and other authorized users to handle the communications needs of the three types of networks. The three networks are the Demilitarized Zone (DMZ), Extranet, and Intranet, the internal State Backbone.

The DMZ is the network outside of the state's firewall that ties into the state's Internet Service Provider (ISP). Services provided by the DMZ are public web and file transfer protocol (ftp) service. All hosts on this network are considered un-trusted and as such are not allowed to communicate to the internal network.

The Extranet is a network that lies outside of the internal network and inside of the DMZ on a third interface coming from the firewall structure. The Extranet is a protected and partially trusted network designed to facilitate external entities that require connectivity to State agency resources. The Extranet is the only point where external entities are allowed to terminate new-dedicated links to the state network. Another service provided by the Extranet is split domain name service (DNS) to hide internal hosts' names. The internal network (Intranet or State Backbone) is the trusted network inside of the state's firewall structure.

The Intranet ("Backbone" or "internal network") is the network that lies inside of the firewall. All trusted State agency networks are allowed direct connectivity into this

network. Internal networks are traditionally considered fully trusted. Internal firewall devices may be implemented where deemed necessary for added protection.

The Wide Area Network is an extension of the intranet, which is used for connectivity to remote offices. ITN must ensure that the security of the WAN is, at a minimum, compliant with the policies, standards, and procedures outlined in this document.

### **Allowed Inbound Network Protocol/Traffic to the State Backbone**

In order to maintain a balance between security (no access) and functionality (no access controls) there is a middle ground. People physically outside the state's internal network may acquire access to the internal network only through controlled methods. Authorized users may connect to the network through the use of DoIT controlled VPN services, Citrix N-Fuse or dedicated links. All new-dedicated links must terminate on the Extranet. All existing dedicated links must be relocated to the Extranet or a firewall must be installed and configured on existing links to protect the state from networks that are not trusted.

The following is a list of the supported computer communications allowed from the Internet into the internal State network. As technology and agency needs change, this list may be modified as needed.

- Mail – generic SMTP mail that traverses on TCP/IP port 25 is allowed into the state network
- VPN connections with user authorization from a single remote host to internal resources. DoIT will maintain an approved VPN service for use by all state agencies.
- Specific traffic that originates on the State's Extranet requires a proxy server to gain access into the internal State network (e.g. webmail, Citrix nFuse) DoIT will maintain an approved Citrix nFuse service for use by all state agencies
- RAS with dial back – DoIT will maintain a remote access server that “dials the user back” as the authentication process. This service will be maintained for use by persons who do not have access to the internet in their remote location until such time as there is no longer a need. It is NOT a preferred technology and agencies are encouraged to use either VPN or Citrix nFuse, if Internet connectivity is available

If an agency is currently using a remote access solution that is not listed above, it must be reported to ITOC for approval. If the solution in use provides adequate protection of the agency network and the State backbone then this system will be grand fathered. If grand fathered, the agency will have a security policy that details the setup, maintenance and management of their remote access solution. However, if it is not providing the security required to protect the state or agency network, the agency will need to bring their current solution to compliance or replace it with an approved service. The decision to upgrade or replace will be based on cost, business need, and ability to secure.

## **Allowed Inbound Network Protocol/Traffic to the Extranet**

The Extranet exists to provide network connectivity between outside un-trusted networks and the internal trusted network. The lists below contain the services currently allowed on the Extranet. As technology and agency needs change, these lists may be modified.

- Supported computer communications allowed from the Internet into the State's Extranet network:
  - Mail – generic SMTP mail that traverses on TCP/IP port 25
  - HTTP (web) – generic web access on TCP/IP port 80
  - HTTPS (secure web) – generic secure web access on TCP/IP port 443
  - VPN connections with user authorization from a single remote host or remote network to specific Extranet resources
  
- Supported computer communications allowed from the internal state network into the State's Extranet network:
  - Mail – generic SMTP mail that traverses on TCP/IP port 25
  - HTTP (web) – generic web access on TCP/IP port 80
  - HTTPS (secure web) – generic secure web access on TCP/IP port 443
  - VPN connections with user authorization from a single remote host or remote network to specific Extranet resources
  - Telnet – generic telnet TCP/IP port 25 or TN3270 to specific Extranet resources from the internal state network
  - FTP – generic ftp TCP/IP ports 20/21 to specific Extranet resources from the internal state network
  - ICMP – generic PING to specific Extranet resources from the internal state network
  
- Supported computer communications allowed from dedicated connections that terminate on the Extranet:
  - Mail – generic SMTP mail that traverses on TCP/IP port 25
  - HTTP (web) – generic web access on TCP/IP port 80
  - HTTPS (secure web) – generic secure web access on TCP/IP port 443
  - VPN connections with user authorization from a single remote host or remote network to specific Extranet resources
  - Telnet – generic telnet TCP/IP port 25 or TN3270 to specific Extranet resources from the internal state network
  - FTP – generic ftp TCP/IP ports 20/21 to specific Extranet resources from the internal state network

## **Allowed Outbound Protocols**

By default the state will allow all needed outbound traffic unless it poses a security risk that outweighs the benefit of allowing the connectivity.

## **Wireless Network Connectivity**

### **Introduction**

Wireless technology is an emerging technology that can provide a more cost efficient means of connectivity, dependent on the method of implementation. The state must clearly understand all implications that a wireless technology will have on the state's resources.

### **Policy**

Wireless connections to the state's networks are prohibited unless expressly approved by ITOC. A task force has been formed to address the wireless connectivity architecture, policy and standards. The wireless architecture task force, comprised of members of state agencies, will review and approve all wireless implementations.

## **Intrusion Detection**

### **Introduction**

There are several tools that can be used to assist in the protection of networked systems. Intrusion Detection is a tool that allows the monitoring of networked traffic for the protection of data and systems.

### **Policy**

It is the responsibility of DoIT to monitor for unauthorized intrusions. DoIT is responsible for monitoring and detecting intrusion attempts on the state's backbone and at the network head end (points of ingress/egress to the internal network and the Extranet). DoIT will maintain intrusion detection software, software patches, intrusion detection techniques, and communications with other non-state incident response teams that can be utilized by State agencies. Only trained personnel with an approved background check will be permitted to operate the state's intrusion detection systems for the state. If an agency becomes aware of a successful intrusion, the detection must be reported to the DoIT Help Desk. Failed intrusions need to be compiled on a biweekly report and submitted to DoIT for further review.

The state will attempt to prosecute intruders when ever possible and will not allow security holes on mission critical systems to go uncorrected in order to learn more about the intruder. Unless critical systems have been compromised, DoIT and any involved state agencies will first make an attempt to track intruders before correcting systems.

ITOC has delegated to DoIT the authority to make decisions concerning closing security holes or attempting to learn more about the intruder.

### **Operational Requirements**

DoIT is responsible for:

- Enabling operating system and application software logging on all host and server systems
- Enabling alarm and alert functions, as well as logging, of any firewalls and other network head end and/or perimeter access control systems
- Installing additional monitoring tools such as Tripwire or appropriate software wrappers on all critical servers as a supplement to the activity logging process provided by the operating system. Examples: Domain Name Servers, authentication servers, security servers in the Unix environment, domain controllers and Exchange servers in the Windows NT environment, and any application server, which is considered to be mission critical, should be afforded this protection
- Reviewing audit logs from the perimeter access control systems daily
- Reviewing audit logs for servers and hosts on the internal, protected network on a weekly basis
- Reviewing audit logs for mission critical servers and hosts on the internal protected network daily
- Monitoring Network traffic. IDS systems will be checked on a periodic basis for proper function and configuration
- System integrity checks of the firewalls and other network perimeter access control systems must be performed on at least a monthly basis
- Reviewing all trouble reports received by system administration personnel for symptoms that might indicate intrusive activity
- Reporting all intrusion detections to the local Infragard Organization and/or the local FBI office
- Installing, at logical network concentration points, IDS tools which monitor for traffic patterns consistent with known attacks

Agencies are responsible for:

- Installing additional monitoring tools such as Tripwire or appropriate software wrappers, on all critical servers as a supplement to the activity logging process provided by the operating system. Examples: Domain Name Servers, authentication servers, security servers in the Unix environment, domain controllers and Exchange servers in the Windows NT environment, and any application server, which is considered to be mission critical, should be afforded this protection
- Training users to report any anomalies in system performance to their system administration staff
- Reviewing all trouble reports received by system administration personnel for symptoms that might indicate intrusive activity

- Documenting and tracking inappropriate computer use

## **Firewall**

### **Introduction**

Firewalls are hardware or software tools used to provide frontline protection for the network infrastructure. A firewall must be properly installed and maintained to ensure adequate protection of the state's network infrastructure.

### **Policy**

DoIT will maintain all Firewalls for the state backbone. They will maintain a firewall structure to protect the state's networks for unauthorized access over the state's connection to the Internet. Only trained personnel with an approved background check will be permitted to operate the firewall structure for the state. All setup and implementation criteria will be documented and filed in a safe location.

Changes to the firewall shall be requested and approved utilizing the firewall Change Request Form (appendix C). All changes will require the business justification as well as the IP address (s) and port(s) requiring the change. Approval will be given once all security aspects have been thoroughly checked.

Personal computers that utilize a broadband connection such as DSL or cable modem is in a constant open state to the internet when powered on, providing a vulnerability to the pc as well as any other system it may have connectivity with. Employees that utilize a broadband connection to communicate with the state backbone will have a personal firewall installed that meets or exceeds the state standard.

### **Operational Requirements**

The firewall structure will provide the following general protective functions:

- Block unwanted traffic. By default the firewall blocks all traffic
- Direct incoming traffic to more trustworthy internal systems
- Hide vulnerable systems, which can not easily be secured from the Internet
- Log traffic to and from the internal networks
- Hide information such as system names, network topology, network device types, and internal user ID's from the Internet

- Provide more robust authentication than standard applications or operation systems might be able to do

## Router / Switches

### Introduction

Routers and switches provide the network with added security through directing network traffic to specific IP addresses on the network and disallowing defined IP addresses from being accessed. Routers and switches, like firewalls, require a well-defined policy, standard and installation procedures to protect the network.

### Policy

All agencies that are responsible for the implementation and maintenance of network routers or switches will have a policy to cover their security. The policy will provide the proper setup methodology used, port assignments and maintenance schedule. The policy will be documented and stored in a secure location. The purpose of the policy is two fold. First, it will provide a documented means for additional routers to be setup in a similar manner. Second, the information will be available for use with the agencies disaster recovery plan.

### Operational Requirements

Guidelines for both routers (internal and perimeter) and switches:

- Remote access (i.e. over TELNET): should be handled by a TACACS+ or RADIUS authentication server. This is a secure, central host for accounts/passwords. As well, the Telnet login is restricted to specific administrative users using an access list
- Privileged access: all privileged access passwords should use the enable secret command. This command uses MD5 for password hashing to encrypt the password. Since it is vulnerable to dictionary-based attacks, access to configuration files will be limited to trusted individuals/administrators
- Console port access: This should be similar to the Telnet access. The only method used for console access will be through a direct connection with a console cable. Only privileged administrators are allowed physical access to routers
- Warning Banners: Banners can possibly help with prosecution in the event of an attack. The message of the day (motd) banner which is displayed once the Telnet session is established
- Logging: Logging levels are set to informational so all traces of access and configuration changes are recorded. The routers have buffers to store log

messages locally. Logging will be set to a remote server for centralized storage and to eliminate the possibility of log messages being altered due to a break in

- These services are disabled
  - **No service finger!** Disable the ability to see who is logged onto the router
  - **No service udp-small-servers!** These rarely used services can be exploited
  - **No service tcp-small-servers!** DoS attack
  - **No ip source-route!** This is disabled to prevent spoofing and DoS on older IP implementations
  - **No ip bootp server!**
  - **No ip http server!** Disable the web-based access to router
  - **No logging console!** Save cpu cycles.
  - **No ip directed-broadcast!** This is disabled to prevent SMURF attacks
  - **No ip unreachable!** Disabled to hinder the ability of an attacker to map the network interfaces

## SNMP

SNMP community strings are setup to be difficult to crack. An access-list is also setup to allow only certain hosts to retrieve SNMP MIB information.

Physical access: All routers and switches are located behind key/card or card only access doors. Keys and cards are distributed accordingly.

## Perimeter Router Access

### INBOUND Access-Lists

- These access-lists are necessary for the first line of defense perimeter router.
  - Deny packets with private addressing
  - Deny packets with local host, broadcast and multicast addresses
  - Deny packets without IP address
  - Allow only packets that are part of an established connection
  - Log anything that does not meet the above criteria

### OUTBOUND Access-Lists

- Deny internal hosts from reaching private, broadcast, multicast and all 0 addresses

### Switch Access

- Ports: Unpopulated ports are disabled to discourage non-administrative users from randomly accessing open switch ports. If the non-admin user is aware of the IP subnet or the LAN is using DHCP, they can easily get themselves on the network

- MAC-level access-lists: If requested, ports can be configured with the MAC address of the connected host. This way no other NIC could be connected to the port and roam the network

## Virus Protection

### Introduction

The use of malicious code is on the rise and places all unprotected networks at risk of infection. In order to protect the state's computer resources from these viruses and worms, anti-virus software is required.

### Policy

In accordance with Information Technology Policy (ITP 00-3) Anti-virus protection is required for all network servers, desktops, laptops, and personal computers that connect to the backbone. This includes any personal computers utilized by employees used to connect to the state backbone via the extranet, VPN, or Citrix nFuse.

### Operational Requirements

- No executable files should be downloaded from POP3 or SMTP accounts
- Mail from POP3 accounts, personal accounts, should not be downloaded onto state resources
- All floppy disk carried into or out of the state will be scanned for viruses prior to use in state resources
- All messages received from an unknown source should be deleted or scanned prior to opening
- Anti-virus software will be updated on a weekly basis to ensure the latest .dat files are installed, more frequently if warranted
- Personal computers utilized to communicate with the state backbone will have virus protection that meets or exceeds the state standard

## Protection for the Privacy of Personally Identifiable Data

### Introduction

Privacy is a fundamental right; it speaks to our individual freedom. Data on constituents, personnel, and private contracts, etc. must be secured and protected to ensure privacy and confidentiality when it is electronically stored, maintained or transmitted. Electronic transmissions would include transactions using all media even when the information is physically moved from one location to another using magnetic

tape, disc, or compact disc media. Transmissions over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaboration parties), leased lines, dial-up line, and private networks are all included. Federal and State laws regulate privacy, particularly as they relate to the privacy of individually identifiable health information.

## **Policy**

A policy is a statement of information values, protection responsibilities, and organization commitment for a system. The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. Agencies shall develop policies to protect the privacy of constituent data when applicable. All agencies shall abide by IC 4-1-6 in the collection and use of personal information.

## **Operational Requirements**

- Organizational Practices:
  - Security and confidentiality policies
  - Information security officers
  - Education and training programs, and
  - Sanctions
- Technical Practices and Procedures:
  - Individual authentication of users
  - Access controls
  - Audit trails
  - Physical security and disaster recovery
  - Protection of remote access points
  - Protection of external electronic communications
  - Software discipline, and
  - System assessment

## **Protection of Software and Other Copyrighted Material**

### **Introduction**

The development of software is a time consuming expensive endeavor for any organization. Courts have found organizations and their officers liable for copyright infringement where unauthorized copies were used to the organization's benefit – even when the copying was done without management's knowledge.

## **Policy**

All agencies will develop and implement a policy that directs its employees to comply with copyright laws.

### **Operational Requirements**

The policy should convey, at a minimum:

- That agency policy will notify employees they are required to comply with copyright laws
- Documents or software protected by copyright may only be copied with the written permission of the copyright holder
- Any unauthorized reproduction of the copyrighted material may subject the responsible employee to disciplinary action, civil liability, or both
- The state and/or agency is not obligated to defend or indemnify employees in actions based on copyright violation

The agency policy may include statements such as the following suggested by the Software Publishers Association:

- “(Agency) licenses the use of computer software from a variety of outside companies. (Agency) does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.”
- “With regard to use on local area networks or on multiple machines, (Agency) employees shall use the software only in accordance with the license agreement.”
- “(Agency) employees learning of any misuse of software or related documentation within the (Agency) shall notify [Agency management].”
- “According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as \$100,000, and criminal penalties, including fines and imprisonment. (Agency) employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination. (Agency) does not condone the illegal duplication of software.”

## **Information and Data Sharing**

### **Introduction**

Due to the overall business of state government the sharing of information and or data is a necessity. Many outside organizations as well as state agencies need the information and data that is maintained within the state network to accomplish their

business objectives. This sharing of information and or data does not alleviate the need for adequate security protection.

### **Policy**

All agencies will establish and maintain a Chain of Trust Agreement with any internal or external organization they share information and or data. The Chain of Trust Agreement will as a minimum ensures all parties will utilize the same level of security required by the information and or data as determined by the provider, the timeline for sharing information and or data, and the type of information and or data being shared. See Appendix D for sample Chain of Custody Agreement.

## **Computer Use Policy**

### **Introduction**

The computer hardware and software used by each employee of the state is the sole property of the state of Indiana and the constituents. The equipment is provided to the employees to assist in the completion of his or her duties. The Ethics commission has implemented a diminimus use policy, which agencies can adopt or choose not to adopt. The computer use policy is frequently the first introduction to employee security awareness.

### **Policy**

In accordance to Information Technology Policy (ITP 00-8), a Computer Use policy is required for all state employees and contractors. The computer use policy should include employee security responsibilities on computer use, data use, and software use. Each agency will have signed copies of the computer use agreement by each employee and or contractor.

## **Personnel Security Practices**

### **Introduction**

Security starts with each individual employed by the state of Indiana. It is the responsibility of the employees to ensure all the state resources are protected from internal and external threats.

### **Policy**

State agencies will develop, document, and implement security standards and procedures for employee or contractor selection, orientation, and supervision. The objective is to ensure that a high level of integrity and satisfactory staff conduct is

achieved and maintained, and to promote an awareness of security matters. The personnel security practice policy will be embedded in the human resources standard operating procedures for state employees as well as this security policy.

### **Operational Requirements**

The following should be included as a minimum:

- Hiring practices - Define acceptable levels of prior performance consistent with the sensitivity of the planned work assignment. Consider checks with former peers and/or supervisors at places of prior employment, as well as with references provided
- Background checks - Background checks that include education and previous employment may be considered for selected personnel who will be required by their job to have access to sensitive information

Security Awareness Training - Develop a formal security orientation and training program for all employees. The program should be current and comprehensive consisting of:

- Applicable laws and/or rules
- Importance of Security
- Applicable state policies and standards
- Agency security policies, plans, and procedures
- Employee performance requirements
- Provide specific supervision for new employees working in sensitive areas or on sensitive processes
- Ensure appropriate separation of responsibility and adequate audit trails in sensitive functions
- Vendor and service personnel monitoring
- Establish procedures for orientation and monitoring of the activities of contractors and service personnel
- Potential sanctions for non-compliance
- Termination process

## **Physical Security**

### **Introduction**

Security encompasses many tools and techniques to provide protection; this includes the physical security of computer resources. Data Centers must guard against unauthorized personnel; laptops and workstations must be protected from theft or vandalism. A well-defined and implemented physical security plan and policy will assist in this endeavor.

## **Policy**

State agencies must establish physical security controls over large computer, minicomputer, and microcomputer equipment consistent with the criticality of the equipment. Agencies must document the current physical security standards and make improvements as they relate to:

- Controls over tape files, diskettes, and other media to prevent unauthorized use or removal from IT resource areas
- Procedures for storing and controlling tape files, diskettes, or other removable media
- Specifying labels, volume and serial numbers, and other identifiers consistent with the computer operating system are used for all files
- Outlining the procedures for implementing retention schedules as required by the Commission on Public Records
- Establishing access authorization and modification policy and procedures
- Conduct periodic security access checks on personnel

## **Incident Response**

### **Introduction**

The reaction taken to a potential intrusion and or malicious act, and how quickly these steps are taken will determine what level of destruction occurs. Proper procedures must be in place that directs each individual to the proper action and process they must take to mitigate damage once an intrusion and or malicious act is discovered.

### **Policy**

All agencies will develop Incident Response procedures. The procedures will at a minimum include:

- What anomalies to be looking for
- Who and when to report potential attacks
- What not to do if an intrusion and or malicious attack is discovered
- When to escalate to the next higher authority

## **Off-site storage and environmental controls**

### **Introduction**

Back-ups of network systems provide added protection in case of successful attacks and or disaster. However, the media in which the back-ups are stored needs protection from potential security breach and or disaster as well as the environmental changes that can affect the life of the media. Off-site storage with appropriate environmental controls will provide this security.

## **Policy**

All agencies will develop and maintain back-up procedures. These procedures will include the proper off-site storage requirements needed to protect and safeguard the data and media used for the back-ups.

## **Operational Requirements**

Minimum requirements are to:

- Ensure that storage security needs will be satisfied through use of guards, TV monitors, third-party surveillance, and/or automated security systems
- Ensure that storage-building environment provides adequate protection from fire, electrical problems, civil disturbance, and natural disasters

## **Business Continuity/Disaster Recovery Plan**

### **Introduction**

The following existing policies are reiterated within this document to underscore the importance of appropriate Business Continuity and Disaster Recovery planning to ensure continuation of essential government services. Each agency should have an IT disaster recovery plan that addresses recovery of information technology resources necessary to the continued provision of essential citizen services. These plans should be tested on a regular basis.

The Division of Information Technology (DoIT) holds a contract with Sunguard that may be used by any state agency for Disaster Recovery consulting, planning, and implementation services.

### **Policy**

The State Board of Accounts "Accounting and Compliance Guidelines Manual for State Agencies" states,

"A written Disaster Recovery Plan is required to ensure that critical accounting information will be processed in the event of interruption of computer processing capability. The plan must be updated and tested annually or when significant modifications to computer hardware, software or application systems occur. One copy of the Business Continuity Plan must be retained off-site."

Additionally, the State Emergency Management Agency's (SEMA) Comprehensive Emergency Management Plan states,

- Each department, agency and commission of state, county, city, town and township are responsible to have a continuity plan
  - Designating lines of succession and delegating authority for the successors
  - Establishing provisions for the preservation of records
  - Developing procedures for the relocation of essential departments
  - Developing procedures to deploy essential personnel, equipment and supplies
- Each state agency and each local jurisdiction will include this information in its Standard Operating Procedures, guide or plan
- Additional plans and or documentation include
  - Application and critical analysis
  - Data backup Plan
  - Testing and Revision procedures

## Surplus Computer Equipment and Media

### Introduction

The data and information stored on local hard drives of any workstation is a permanent recording unless cleaned properly using appropriate software tool sets. There are special software applications that can render a hard drive clean by wiping all information stored on the drive. The Delete function within the Windows operating system does not adequately perform this task.

### Policy

All data and programs should be removed from electronic storage media by the agency before being sent to State Surplus, moved to another agency, donated, and or destroyed. Failure to protect Individually Identifiable information on constituents is cause for employee sanctions. A log will be maintained that provides an audit trail of destruction. Minimum information required for log will be name of person destroying information, the physical device name, date destroyed, hard drive manufacturer and serial number.

### Conclusion

The protection of the states information systems resources and data is part of every employee's responsibilities. This policy is meant to be a minimum requirements document; each agency should use at their discretion in building their agencies security plans and policies. If an agency deems it necessary to add more stringent security measures they may do so, as long as the policy supports the measures deployed.

## Appendix A

Before an agency can develop a sound security program there are several steps that need to be accomplished. The following outline provides a plan that can be followed to best develop an overall security program for the agency. There is a lifecycle to any good system and security is no different. The lifecycle for security that needs to be considered when planning a program is Develop a Plan, Develop Policies, Develop Procedures, Enforcement, Management of the Process, Detection, and Assessment. Security is an ever evolving initiative that changes and must be maintained to be effective.

- **Determine Current Security Posture**
  - What policies are in place
  - What hardware / software is currently being used for security
  - Is there Dial up connections? How are they secured
  - Is there a security manager for the agency
  
- **Review the Enterprise Security Policy Guidelines**
  - Compare to current security posture
  - Determine what agency requirements are
  - Determine what security solutions are already being accomplished
  - Determine what security solutions/policies need to be implemented
  
- **Develop Security Plan**
  - Ask the following question
    - What are you trying to protect
      - Identify the object
      - Classify the object based on mission criticality
      - What value would you place on this object based on criticality to mission. How much monetary loss would occur if not available
    - From whom are you protecting the object
      - Internal entities are the number one security threat
      - What external entities would be a threat
    - How do we balance security in relation to
      - Risk vs. cost
      - Accessibility vs. security
    - What do we do if a security violation happens
    - How do we educate the employees
  - Plan for implementation and budgeting for security
  - Document plan to address agency security requirements
    - Define security requirements
    - Define agency security mission and vision
    - Define stakeholders in your security initiative
    - How long will it take to implement plan
    - If required

- Purchase hardware and software
  - Develop agency specific policies and procedures
  - Train security personnel
  - Develop agency educational program
- Consider continual improvement concept in plan
- **Review Plan for completeness**
- **Forward Plan to ITOC for review**
- **Implement plan**
- **Maintain the security plan (renew this cycle each year)**
  - Review the current security plan
  - Compare the plan to the enterprise security policy guidelines
  - Revise the security plan accordingly
  - Review the revised security plan for completeness
  - Forward the revised security plan to ITOC for review
  - Implement the revised security plan

## Appendix B

### AGENCY SECURITY MANAGER

**Position:** Information Security Officer

**Agency:** Division of Information Technology (DoIT)

**Introduction:** A good security program begins with the right person selected to manage the program from all aspects. A security program needs administered on a daily basis. The security officer is that person that must have the authority to ensure security is addressed by the security team and the operational personnel. An effective security program is everyone's responsibility and the central responsibility for the program lies with the security officer and his/her team.

**Responsibilities:** To properly manage/administer a security program the security officer would be responsible for, but not limited to:

- Administrative controls
  - Reporting to the CISO and agency MIS Director
  - Development and publication of agency policies standards, procedures, and guidelines
  - Screening of personnel that will work within the security arena
  - Development of agency training and awareness program
  - Monitoring of systems
  - Development and management of change control process
  - Development of Incidence Response/Computer Forensics team
  - Project Review for Security
- Technical controls
  - Account management
    - Logical access control
    - Password and resource management
    - Identification and authentication methods
    - Security devices and configuration of the agency network
- Physical Controls
  - Access to data center and agency resources
  - Monitoring the intrusion and access controls to the agency
  - Monitoring the environmental controls

The security officer would work closely with the other deputies to ensure operational and security efforts work in a cohesive manner to ensure the services are provided in the most efficient yet secure manner. Reporting to the CISO the security officer would also be responsible assist in the overall security of the state.



# Appendix C

## FIREWALL CHANGE REQUEST

In an effort to provide a more secure networking environment and provide better service to all agencies any changes to the firewall must be submitted in writing. This form is intended for requesting changes and obtaining approval by ITOC. All requests will be routed to DoIT via ITOC for investigation into the security implications and subsequent approval or disapproval.

Requesting Agency:  Date:   
Time Frame:   
Contact Name:  E-Mail Address:

Technological Description: (What changes do you want to be made?)

Description of Business Drivers: (Why are you requesting this change?)

Source Address(es):

| IP Address           | PORT #               | TCP/UDP              |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

| IP Address           | PORT #               | TCP/UDP              |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

Destination Address(es):

| IP Address           | PORT #               | TCP/UDP              |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

| IP Address           | PORT #               | TCP/UDP              |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

Signatures:

\_\_\_\_\_  
Requesting Agency Date  
\_\_\_\_\_  
Department of Information Technology Date  
\_\_\_\_\_  
Information Technology Oversight Commission Date

\_\_\_\_\_  
Requesting Agency (Please Print) Date

Audits are frequently performed on the State of Indiana firewalls. If it is determined that a requested change has not been accessed for 30 days the statement will be removed from the firewall and a new request will need to be submitted.

## APPENDIX D

### CHAIN OF TRUST AGREEMENT FOR TRANSMISSION OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION IN ELECTRONIC FORM

This agreement, is entered into by and between ORGANIZATION, located at \_\_\_\_\_, and \_\_\_\_\_ (PARTNER), located at \_\_\_\_\_.

WHEREAS, it is the benefit for PARTNER to be able to access individually identifiable health information held by ORGANIZATION,

WHEREAS, ORGANIZATION has an obligation to ensure the confidentiality of individually identifiable health information in its care, and further to ensure that it only makes such data available to parties which have an acceptable need to access such data, and

WHEREAS, PARTNER has a need to access specified individually identifiable health information held by ORGANIZATION,

NOW THEREFORE, in consideration of the covenants and conditions set forth in this Agreement, the parties agree as follows:

## SECTION I

### Definitions

- 1.1 AUDIT refers to a formal review and identification of access to an information asset by an individual, organization, or application process.
- 1.2 AUTHENTICATION is the process by which a user (or application process) identifies herself or himself to an information system or resource. The user is required to provide at least one (often a combination) of the following unique elements:
  - 1.2.1 Something that the user knows (such as a password or a personal identification number);
  - 1.2.2 Something that the user has in his/her possession (such as a token or access card);
  - 1.2.3 Something that is characteristic or an expression of the user's physical being (such as finger or voice prints).
- 1.3 DATA refers to the individually identifiable health information, physician information and other proprietary information that has been identified as appropriate for sharing between ORGANIZATION and PARTNER.

- 1.4 ENCRYPTION refers to the reversible conversion of readable information into an unreadable, protected form so that only a recipient who has the appropriate “key” can convert the information back into its original readable form.
- 1.5 INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION means any information held by ORGANIZATION including elements that allow unique identification of an individual, specifically demographic information such as name, address, social security number, date of birth, sex, etc. Individually identifiable health information includes but is not limited to the following examples if they contain such data elements:
- (a) Patient information generated, collected, maintained, or distributed by ORGANIZATION including transferred (medical) records, and all correspondence;
  - (b) Information entrusted by a patients or research subject to an employee, trainee, student, volunteer, vendor, consultant, or member of the faculty or clinical staff;
  - (c) Any knowledge An ORGANIZATION employee, trainee, student, volunteer, vendor, consultant, or member of the faculty or clinical staff has regarding a patient;
  - (d) Research information collected, generated, maintained, or disseminated by ORGANIZATION which identifies individual or when combined with other data can lead to the identification of an individual;
  - (e) Personnel information collected, maintained, or generated by ORGANIZATION that identifies current or past employees other than the information which is made available under Federal or State law, statute, or regulation, or under University policy;
  - (f) Academic information collected, maintained, or generated by ORGANIZATION that identifies current or past students.

## **SECTION II**

### **Rights and Duties of ORGANIZATION**

- 2.1 ORGANIZATION agrees to treat security, personnel, and policy information disclosed to it by PARTNER under this Agreement as confidential.
- 2.2 ORGANIZATION agrees to provide PARTNER with ORGANIZATION policies on confidentiality and data security as well confidentiality statements attesting to the PARTNER’s knowledge of compliance with these policies.

- 2.3 ORGANIZATION will provide PARTNER with individually identifiable health information in the form of \_\_\_\_\_, including but not limited to microfiche, magnetic tape, disk, and by electronic transmission.
- 2.4 ORGANIZATION will determine if PARTNER's security measures are sufficient to protect DATA and recommend changes before releasing DATA.
- 2.5 ORGANIZATION agrees to designate a point of contact for PARTNER.

### **SECTION III Rights and Duties of PARTNER**

- 3.1 PARTNER understands that the information it will receive is confidential and PARTNER agrees to maintain and protect the confidentiality of all information it has access to as a result of this Agreement, Section 8.1.
- 3.2 PARTNER agrees to disclose the security measures it uses to protect the DATA, which must meet applicable professional standards.
- 3.3 PARTNER agrees to provide the names and job titles of all its personnel who are given access to DATA, and its disciplinary procedures regarding breaches of computer security and confidentiality, to ORGANIZATION upon request. PARTNER agrees to update Appendix A with every addition or deletion of any staff member to have access to DATA.
- 3.4 PARTNER agrees to distribute ORGANIZATION Confidentiality and Data Security Policies to employees with access to individually identifiable health information, Appendix B, and require that each employee with access to ORGANIZATION DATA sign confidentiality statements attesting to his/her knowledge and compliance with those policies, Appendix C.
- 3.5 PARTNER agrees to retain copies of each employee's confidentiality statement attesting to his/her knowledge and compliance with the ORGANIZATION Confidentiality and Data Security Policies and present these statements to ORGANIZATION upon request.
- 3.6 PARTNER agrees to (\_\_\_\_\_) information provided by ORGANIZATION to the form of including but not limited to microfiche, magnet tape, disk, and by electronic transmission.
- 3.7 PARTNER agrees to report breaches of security to ORGANIZATION as soon as possible in order to minimize damages.

### **SECTION IV Systems Operations**

4.1 Each party, at its own expense and its own site, shall provide and maintain the equipment, software services and testing services necessary to effectively convert, process or interchange DATA in the form of including but not limited to microfiche, magnetic tape, disk, and by electronic transmission and ensure the integrity of all DATA converted, processed, or interchanged.

4.2 PARTNER shall allow ORGANIZATION or its designee to review PARTNER's security of external DATA within normal business hours.

4.3 PARTNER agrees to designate a point of contact from ORGANIZATION.

4.4 PARTNER agrees to receive written permission from ORGANIZATION before outsourcing any work identified in this Agreement to a subcontractor.

4.5 PARTNER agrees to ensure that subcontractor will maintain the security and confidentiality provisions of this Agreement.

4.6 PARTNER agrees not to copy the individually identifiable health information in any media, except that necessary to complete the process of transferring the DATA in the form of including but not limited to microfiche, magnetic tape, disk, and by electronic transmission.

## **SECTION V Ownership**

5.1 ORGANIZATION is the guardian of all DATA rights and information contained within the records shared with PARTNER. Each individual about whom information is shared with PARTNER is the owner of all DATA rights and information that is being shared.

5.2 PARTNER covenants not to enter into any agreement allow any other party to view or extract DATA in any form from all information placed in PARTNER's care, without the written consent of ORGANIZATION.

## **SECTION VI Compensation**

6.1 ORGANIZATION agrees to compensate PARTNER in accordance with the terms of the RFP.

**SECTION VII**  
**Term and Termination**

- 7.1 The term of this Agreement shall be for a period of \_\_\_\_\_, commencing on \_\_\_\_\_, 1999.
- 7.2 This Agreement may be renewed for an additional year by written notice of renewal signed by both parties.
- 7.3 The procedures for termination of this Agreement, for any reason, will be as follows:
- a) PARTNER will return all DATA, regardless of media, or ORGANIZATION.
  - b) PARTNER agrees to destroy any and all copies in any medium, physical or electronic, that were created to transfer the DATA including but not limited to magnetic tape, microfiche and electronic transfer so that none of the individually identifiable health information, physician information and other proprietary information can be retrieved or replicated.
  - c) PARTNER shall make available to ORGANIZATION all services necessary for an orderly transfer of PARTNER's obligations under this Agreement at the time of termination of the Agreement.

7.5 This Agreement shall immediately terminate, at the option of ORGANIZATION, if:

- a) Any petition in bankruptcy is filed by or concerning PARTNER. In no event shall this Agreement become an asset in any such proceeding nor shall ORGANIZATION or the University of ORGANIZATION be bound by this Agreement, after any act of bankruptcy by PARTNER. Any delay by the University or ORGANIZATION in the exercise of the right to terminate this provision shall not diminish or waive this right.
- b) Any breach of confidentiality.

**SECTION VIII**  
**Other Important Provisions**

8.1 Confidentiality. PARTNER understands the, <Name of State> and Federal laws on confidentiality of medical records and other individually identifiable health information and shall ensure that its staff is properly trained in the handling of medical records and other individually identifiable health information under State and Federal law and the ORGANIZATION policies.

- 8.1.1 PARTNER understands that individually identifiable health information may only be released by authorized ORGANIZATION employees, in accordance with the terms of this Agreement.
- 8.1.2 PARTNER shall ensure that the individually identifiable health information that is released to PARTNER will be kept confidential and will not be used by PARTNER or its agents, representatives, or employees, and shall indemnify the University for all payments, legal fees, and costs incurred by such breach.
- 8.1.3 PARTNER shall be responsible for any breach of confidentiality by its agents, representatives, or employees, and shall indemnify the University for all payments, legal fees and costs incurred by such breach.
- 8.1.4 In the event of such a breach, PARTNER will immediately notify ORGANIZATION of the specifics.
- 8.1.5 PARTNER and its officers, employees and agents understand that confidentiality shall survive the terms of this agreement.
- 8.2 Security. Each party shall use those security procedures, which are specified in Section III, to ensure that all transmissions of DATA are authorized and to protect ORGANIZATION medical records and DATA from improper access. When information must travel across lines of communication where both ends are not under the control of the Regents of the University of <Name>, PARTNER agrees to use, at a minimum, strong authentication and encryption to protect the DATA.
- a) PARTNER will use security/access software and/or procedures sufficient to reasonably ensure that all transmissions of DATA are authorized and to protect the DATA from unauthorized access.
  - b) PARTNER will safeguard the DATA from tampering and unauthorized disclosures. This protection must extend beyond the initial information obtained from ORGANIZATION to any databases or collections of DATA containing information derived from the DATA. This provision shall be in force even if DATA are made anonymous by removing any identifying information. PARTNER shall maintain the confidentiality of passwords and other codes required for accessing this information.
  - c) PARTNER may not sell, release, or otherwise furnish such information to any third parties without the written approval of ORGANIZATION.
  - d) Access is limited to authorized personnel as specified in Appendix A and referenced in Section 3.3.
  - e) The list of authorized personnel in Appendix A may be amended from time to time with the permission of ORGANIZATION.

8.3 Notices. All payments, notices and formal communications required or permitted under this Agreement shall be made in writing and shall be deemed to be duly given if sent by first class mail, postage prepaid, return receipt requested, addressed appropriate as follows:

**PARTNER:** \_\_\_\_\_ **ORGANIZATION** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

8.4 Assignment. In no event shall either party assign any of its rights, powers, duties or obligations under this Agreement without the prior written consent of the other party; provided, however, that ORGANIZATION and PARTNER may assign all or part of this Agreement to its successor, affiliated, and assigns.

8.5 Severability. If any provision of this Agreement is held invalid by a court of competent jurisdiction, such provision shall be deemed modified to eliminate the invalid element, and as so modified, such provision shall be deemed a part of this Agreement. If it is not possible to modify any such provision to eliminate the invalid element, such provision shall be deemed eliminated from this Agreement. The invalidity of any provision of this Agreement shall not affect the force and effect of the remaining provisions.

8.6 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the State of ORGANIZATION.

8.7 Enforceability. This Agreement shall be enforceable only by the parties hereto and their successors in interest by assignment. No other person shall have the right to enforce any of the provisions contained herein nor is this Agreement intended to create any third-party beneficiary rights.

8.8 Amendments. This Agreement may not be revoked, altered, changed, modified, amended or discharged except in writing. No waiver of one or more of the provisions of this Agreement or failure to enforce the Agreement by either of the parties hereto shall be construed as a waiver of any subsequent rights. Only the signatories to this Agreement, or their successors, may revoke, alter, change, modify, amend, or discharge this Agreement.

8.9 Prior Agreements, Modifications. This Agreement, together with any attachments, exhibits or appendices, constitutes the entire agreement between the parties regarding its subject matter and shall supercede all prior agreements, promises, negotiations, and representations, oral or otherwise with respect to this subject matter.

8.10 Indemnification. PARTNER agrees to indemnify and hold harmless the Regents of the University of <State>, its governing board, from and against any and all claims, costs, losses, damages, liabilities, expenses, demands, and judgments, including litigation expenses and attorney's fees, which may arise from PARTNER's performance under this Agreement or negligent acts or omissions of its subcontractors, agents, or employees.

- 8.11 Liquidated Damages. PARTNER agrees that ORGANIZATION would be substantially and irretrievably damaged by PARTNER sharing any of the individually identifiable health information, in any form, provided to PARTNER with any other party. PARTNER shall be personally responsible to pay ORGANIZATION the amount of \$50,000.00 in liquidated damages per occurrence should the PARTNER or any of its subcontractors, agents or employees intentionally or accidentally make available any DATA to another party.
- 8.12 Injunction. ORGANIZATION shall be entitled to obtain an injunction against PARTNER in a court of competent jurisdiction should PARTNER share the individually identifiable health information, in any form, provided to PARTNER with any other party. PARTNER shall be responsible for payment of ORGANIZATION legal fees and costs associated with obtaining such injunction.
- 8.14 Insurance. PARTNER agrees to maintain, at all times relevant to this Agreement, insurance in a form and in limits acceptable to the University. Required are: commercial general liability insurance, including contractual liability, with limits not less than \$2 million per occurrence and \$3 million annual aggregate and errors & omissions insurance with limits not less than \$2 million per occurrence and \$3 million annual aggregate. Evidence of such insurance shall be provided to ORGANIZATION upon request and 30 days prior written notice of a reduction in stated limits or cancellation of stated insurance will be provided to ORGANIZATION.

IN WITNESS WHEREOF, THIS AGREEMENT IS EXECUTED by the parties, by their duly authorized representatives as of \_\_\_\_\_ day of \_\_\_\_\_, 2001.

**REGENTS OF THE UNIVERSITY  
OF <State>**

**PARTNER NAME:**

By: \_\_\_\_\_  
Title: \_\_\_\_\_

By: \_\_\_\_\_  
Title: \_\_\_\_\_

Appendix A

*Authorized Personnel to Access Data*

This list may be amended from time to time with the permission of ORGANIZATION.

| Name | Position | <b>Date</b><br><b>Educated</b><br><b>In Laws and</b><br>ORGANIZATION Policies | <b>Date</b><br><b>Confidentiality</b><br><b>Statement</b><br>Signed | <b>Date</b><br><b>Access Access</b><br>Provided | <b>Date</b><br><b>Terminated</b> |
|------|----------|---|---|---|----------------------------------|
|------|----------|---|---|---|----------------------------------|



## *Appendix C*

### UNIVERSITY OF ORGANIZATION HEALTH SYSTEM

#### Confidentiality Statement

In consideration of the University of ORGANIZATOIIN Health System (ORGANIZATION) agreeing to provide certain confidential information to \_\_\_\_\_ Company and its employees, \_\_\_\_\_ Company and each employee provided with confidential information agree to abide by the terms of this statement.

A. Patient care information, whether in written, unwritten, or electronic computer system form, may be access only by ORGANIZATION employees or contracted personnel who need that information to perform their job or contractual responsibilities. Patient care information may only be released to individuals outside the health system by authorized ORGANIZATION employees.

B. I understand that this information belongs to the patient and I am only the caretaker and must guard the information appropriately. This includes, but is not limited to, keeping patient information secure, private, and out of public viewing, protecting computerized data by logging off when leaving a work station, and keeping information secure by not discussing patient-specific issues in public areas such as elevators, etc.

C. Contracted personnel may only access data necessary to perform their contracted responsibilities. Contracted personnel agree not to disclose, communicate, or use any patient care information in any manner whatsoever other than in the provision of contracted services and, even within the scope of those services, must limit dissemination to those who have signed confidentiality agreements and have a need to know.

D. Contracted personnel agree not to copy or download this confidential information. If for some reason confidential information must be copied, the contracted personnel must obtain permission from ORGANIZATION employee and must return such information to ORGANIZATION immediately after completion of that particular activity.

E. The confidentiality of this information survives the termination of your contracted personnel status.

F. I understand that if I do not keep patient information confidential, or if I allow or participate in the inappropriate dissemination of or access to patient care information, my employer will be sanctioned \$50,000 per infraction and criminal offenses will be reported to the proper authorities.

*(Note: often the vendors would like to remove F)*

G. Contracted personnel agrees to comply with all state and federal laws applicable to the use of this confidential information.

My signature attests to the fact that I have read, understand and agree to abide by the terms of this statement and the University of ORGANIZATION Health System's policies on confidentiality of patient care information (policy #03-07-015)

Name: \_\_\_\_\_

Contracting Company \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_