March 31, 2005

Open letter to all interested in security

RE: **Security Policy Tool Kit**

Dear Policy Managers and Security Professionals;

The attached document was developed by a team of Banking Regulatory Agencies utilizing references they believed reliable, educational and worthy of consideration. However the team believes more than a document is necessary to appropriately measure and mitigate risk and thus this *Security Policy Tool Kit* came to life.

CSBS – Best Practices - Security Policy Tool Kit provides a process, which if followed, will result in an orderly internal review of asset identification, vulnerability management, risk mitigation and security monitoring. The *Security Policy Tool Kit* was designed by regulators for regulators; however, several examiners within the development group felt the *Kit* would also be productive for bankers. Utilization of the *Security Policy Tool Kit* is free; however, CSBS Best Practices craves feedback. Whether the *Kit* worked to increase security awareness or failed, CSBS Best Practices would like to know.

Each member of the Information Security Committee professionally expresses opinions regarding financial and IT risk, regulation and fiduciary responsibility. Based upon years of experience, the Committee believes a committed group process will generate a better Security Policy and better security. Finally, the Committee wishes each agency or institution access to reliable resources, industry respect in the "due care" treatment of confidentiality and pride in knowing your service promotes the industry of banking and finance.

CSBS Best Practices,

Information Security Committee

SECURITY - Introduction:

Security is a process, not a lock, firewall or a guard. Thus, simply handing out documents titled security policies would be of little lasting value. The following pages create a process of increasing and recording awareness of threats, vulnerabilities, risks as well as promoting effective countermeasures and detailing the assumed risks.

> The pessimist sees difficulty in every opportunity. The optimist sees the opportunity in every difficulty.
>
> WINSTON CHURCHILL

Additionally, do not spend too much time working on each minute detail at the beginning of this process. Security must be considered as a whole, for just as spending thousands on a door lock when windows do not latch would limit the career of any banker or government employee, the decision to tend a firewall at the main office without monitoring a firewall at a field office can be just as dangerous. Effective security is a philosophy first and an economic activity second. This Kit is designed to assist in building a process that will measure threats to agency assets, design a Security Policy and finally build a Security Plan.

TABLE OF CONTENTS:

BEST PRACTICES:

In a court of law computer records are considered hearsay. If disaster strikes and an agency or bank finds themselves legally explaining security, the parties may look to establishing "due care". This Kit is designed to assist in establishing a process. Best Practice recommends assigning people to each of the following steps listed on this page. The people selected will need to understand they are not conducting a one-time government compliance report; rather they are part of a process. A process that will become a day to day consideration relative to the agency's business practices. Eventually, as the agency periodically cycles through the below steps, reviewing and updating; the policy and plan blend into a "business practice" establishing evidence and confirmation of "due care".

BEST PRACTICES RECOMMENDATION:

A. Periodically, perform a Risk Assessment that serves to increase security awareness.

Process must include:

1. Identify the assets (tangible and intangible) of the agency.
2. Identify the threats to the assets.
3. Identify the methods of risk mitigation or understand risk acceptance.
4. Identity methods of testing mitigation.
5. Perform a Risk Assessment prior to changing technology or processes.

C. Provide a written Security Policy that communicates Management's security strategy to all employees.

D. Provide a written Security Plan to implement the Security Policy throughout the agency's operations.

E. At least annually, review compliance with the security policy and report on its effectiveness to management based upon an updated risk assessment.

SECURITY POLICY:

The Security Policy is a guidance document reflecting management's instructions. Policy should not be written without consideration to the Risk Assessment and the capabilities reflected in the Security Plan. However, if the organization fails to see the vision of security and languishes in the assessment exercise, a policy statement from management offers guidance and structure. While, without an assessment or plan, a policy statement may not offer sufficient day to day detail to safeguard the organization; it does offer instruction regarding day to day considerations.

SAMPLE DIVISION POLICY

> Information maintained by the Department is considered sensitive and/or confidential and for Department use only, except for information specified in the Code of Regulations as public and must be evaluated and protected against all forms of unauthorized access, use, disclosure, modification and destruction. Security controls must be sufficient to ensure the confidentiality, integrity, and availability of important information.
>
> Each employee is required to maintain confidentiality of Department information and provide proper levels of protection to safeguard Department information and electronic equipment under his/her control.[1]

SAMPLE LAPTOP POLICY

> All laptops acquired for or on behalf of the Department shall be deemed state property. Each employee issued a laptop is responsible for the security of that laptop, regardless of whether the laptop is used in a bank, the division headquarters, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport. [2]

A well designed policy addresses:

1. What is being secured?
   Typically an asset.
2. Who is expected to comply with the policy?
   Typically employees.
3. Where is the vulnerability, threat or risk?
   Typically an issue of integrity or responsibility.

Policy may not directly address the When, Why and How.
When – Date policy is signed by the employee.
Why – To protect both the employee and the department from negligence.
How – To be discussed in the "Security Plan".

[1] Special thanks to the State of California, Department of Financial Institutions.
[2] Special thanks to the State of Iowa, Division of Banking.

Risk Assessment:

> The journey of a thousand miles starts with a single step.
>
> LAU TZU

Best Practices recommends beginning the process by generating copies of each of the risk assessment worksheets. Senior management should deliver the worksheets with instructions that each division is to consider those "assets" that deserve security in each of their areas. The worksheets reflect the first steps to promoting a culture where security is a daily consideration; however the worksheets are deliberately not complete. Each worksheet should reflect a listing of tangible or intangible assets and a security approach relative to a field of specialization and/or a unique area of the facility.

Identify the assets of the agency by considering input from the following people or divisions of people:

Worksheet Recipient	Responsibility	Expected Asset Awareness
Division Management	Integrity of the Agency	Information, Reputation, Industry
IT Management	Integrity of Information	Hardware, Software, Topology, Access
Human Resources	Employee Awareness	Employment Agreements, Contracts, Terminations, Confidential Information
Examiners	Examinations	Confidential Information, Laptop Computers
Office Manager	Office workings	Facility, Budget, Operations
Staff	Day to Day	Processes and Resources necessary to get the job done.

Risk Assessment

To be completed by: **Division Management**

Page 1 of _____

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
Reputation	Negligence	Hire the right people – background check? Training – include social engineering? Policies – reflect the business process. Management – security conscious?
Information	Theft Wireless Listening Computer Hacking	Limited access (building, files, data) Encryption in transmission and storage. Up to date Firewall, Antivirus, Spyware definitions.
Obsolete Assets	Lost information	Degaussing of electronic media prior to disposal. Secure paper until shredding. Control over cleaning crews.
Plans	Lack of due care	Security Plan Disaster Recovery Plan Media Plan

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment

To be completed by: **Human Resources**

Page 1 of ____:

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
# FTE	Personal Violence Flu Disgruntled Employees	Emergency procedures posted Health Plan Employee Counseling
Contractors	Theft / Extortion	Limited access – see IT & Mgmt
Cleaning	Theft / Alteration of Records	
Volunteers	Awareness of Confidential Information	
Non-Disclosure Agreement	Failure to sign or violation of terms	
Annually signed agreements	Failure to include security policy & plan	
IT Staff	Misuse of IT resources	
Examiners	Misuse of Exam information	
Staff	Errors Theft Access Misuse of Dept resources	

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment

To be completed by: **IT Management**

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource #	Threat	Mitigating Measure
Main Frame	Access Theft Damage (power surges, air conditioning failure) Destruction Integrity of Information On and On-Line	Password / 8 character / chg 90 days Changes in key fields reported daily UPS, generator Limited access Surge protectors Alarm notification for air conditioning failure / fire/ water Back-up air conditioning system Logs
Servers	Access Theft Damage Destruction Integrity & Loss of Information On and On-Line Updates firmware – software Theft	Limited access Surge protectors Alarm notification for air conditioning failure Back-up air conditioning system Data Backup Logs
Personal Computers	Damage (power surges, air conditioning failure, spilled beverages) Destruction (fire, earthquake, tornado) Theft Remote or Outside access Inappropriate Internal access Integrity and loss of Information.	No liquids on same surface as computer Surge protectors Secure office policy Security software on PC Training of user System time out Chain PC to desk Data Backup Antivirus / spy ware / firewalls
PDA	Theft Damage Destruction Virus Vulnerability	GPS tracking Virus Protection
Laptops	Theft Damage (power surges, spilled beverages) Destruction Security of information	Secure laptop in locking docking station Cable lock Secure unattended laptop in locked cabinet Secure laptop in locked car trunk when traveling Don't check laptop at airport No liquids on the same surface as computer Surge protectors Encryption of information Smart cards Hold user responsible
Printers	Damage Destruction Theft Wrong people pick up job	Surge protectors Secure office policy Assign printers to groups; logically & physical

Risk Assessment

To be completed by: **IT Management**

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
Scanners	Damage Destruction Theft Wrong people picking up scan job	Surge protectors Secure office policy Assigning scanners to groups: ✓ Scanner alone ✓ PC shared scanner ✓ Network scanner
Smartcards	Theft Damage Destruction	Keep smartcard in secure location when removed from computer
Modems	Intrusion and hacking	Replace by VPN
Software (e.g. antivirus)	License location Update methods Renewals Pirated	Protect license key – Store in secure location and have an inventory of software Patch push out Maintain accurate renewal schedules Don't enable loading or downloading software by users Check software inventory whenever a machine is touched
Routers	Intrusion	Logically locking the system
Hubs	Open System	Physically inspect for "hub out connect"
Intrusion Detection	Malfunction	Upgrade definition and patches
Firewall	Intrusion	Blocking & filtering of unknown traffic Review logs
DMZ	Hacking	Eliminating unnecessary services
Web Page	Spoof, hack, part of phishing	Frequent monitoring including web searchers

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment — Wireless Network

Page 3 of ____ To be completed by: **IT Management**

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset/ Resource	Threat	Mitigating Measure
Wireless LAN		
Wireless Access Points	Theft Unauthorized access	Secure office entrance Disallow AP administration via wireless
Wireless Cards	Theft	Less threat in newer laptops since more and more are integrated on board; Secure laptop access by smart card, etc; Lock laptop in trunk when in car
Air space	Man-in-the-middle hack; Radar jamming	Secure office entrance; Tighten up authentication; Configure clients so they only communicate with preferred networks; Disable peer-to-peer wire less network; Identify the network devices
Authentication Server	Theft Unauthorized access	Secure physical access to the server; Secure local server logon with smart card, etc and limit or disable remote logon; Intrusion protection, including termination of infected devices
User authentication	Wireless eavesdrop	Encrypt network authentication traffic; Implement tools, such as smart card,; WPA and 801.1x wireless network, frequent change of wireless session key; Radius server or third-party user authorization software
Data	Unauthorized access	Encrypt air traffic; Secure user authorization on data storage; Secure physical access to the client computers to prevent impersonation or direct access;
Computers equipped with wireless cards	Virus, spyware, etc.; Insecure split-tunnel between two networks	Up to date antivirus/anti-spyware software; Secure all other networks connected to the computer; Up-to-date personal PC firewall; Shutdown unnecessary services

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment — Wireless Network

Page 4 of ____ To be completed by: **IT Management**

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset/ Resource	Threat	Mitigating Measure
Wireless LAN, Bluetooth, etc		
While the device is connected to corporate network, it becomes an extension of wireless LAN	All listed above	All listed above
While offline from corporate network	Eavesdrop and pin stolen	Make sure the length of pin is at least 10 digits
	Tracking within 300 ft range	No solution other than turn off the Bluetooth device

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment

To be completed by: **Office Manager**

Page 1 of _____

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
# of Offices		
Building Access	Fire Flood Contamination Earthquake	Alarms Physical Locks Magnetic Locks (power on/off) Elevator
Building Perimeter	Doors Windows Ceiling Floor Ventilation	
Building Intrusion Detection	Fire Flood Vapors / Gas Unauthorized Access	
Emergency Procedures	Fire Flood Vapors / Gas Unauthorized Access Personal Threat	
Authorized use of Building	Cleaning Staff	
IT Staff	Misuse of IT resources	
Examiners	Misuse of Exam information	
Staff	Errors Theft Access Misuse of Dept resources	
Information	Sharing of confidential information	Clean desk policy Screen savers Locking file cabinets

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment

To be completed by: **Examiner**

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
FI information	Information Breach	Control Copies Degauss disks / drives when finished Maintained Firewall
E-mail	Information Breach	Encrypted transmission
Reputation	Blamed for FI information breach	Standard Exam Practices
Laptop	Theft	Office considered secure? Locked in trunk when in Car? Locked to desk with cable in FI? Is home considered secure? Control during speeches?
Work papers	Tornado Explosion Theft	
Backup files	Damage Theft	
Duplicate files	Loss / Theft	

Add additional sheets as necessary (see blank worksheet at the end of this section).

Risk Assessment

To be completed by: **Staff**

Page 1 of _____

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures that are in place or that should be considered.

Asset / Resource	Threat	Mitigating Measure
Licensing	Unauthorized software	Do not down load Screensavers Games
Screens of Info	Unauthorized viewing	Authorized Screensavers Screen not facing window or public. Spy ware filters.
Phones	Social Engineering	Training
Paper Stock (licenses, checks)	Theft	Lock inside of file cabinet
E-mail address	Spoof	Notify IT
Electronic files		
Paper files		

Add additional sheets as necessary (see blank worksheet at the end of this section).

SECURITY PLAN

The SECURITY PLAN explains the operational details necessary to mitigate the threats listed during the risk assessment while seeking compliance with the Security Policy. A well-designed security plan will promote Confidentially, Integrity and Availability; the CIA of security.

Best Practices suggests at least one planned mitigating issue for every asset listed in the risk assessment. In some cases accepting the risk associated with an asset may be the plan. After consideration to the cost of protecting an asset compared with the likelihood of vulnerability exploitation, the security plan may offer general guidance in the place of specific actions. Regardless of a plan containing absolute actions or general guidance, the purpose of the plan is to convey the understanding to every employee that the agency's assets shall be safeguarded. A Security Plan should consider both the internal response as well as the public's response to issues regarding agency reputation.

SECURITY Plan worksheet

Each of the following areas reflects procedures and/or controls that protect the assets identified in the risk assessment from becoming a victim of exploited vulnerabilities.

Security Plan Worksheet
Page 1 of _____

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*
Building	Security – Opening, Closing & Panic Fire, Flood, Gas Evacuation - earthquake Elevator – access Locks, Latches, Timed Access Cameras , Alarms Car / Airplane crash	Security zones – establish layers of security Locks, latches - reviewed Employee and non-employee access	Are procedures easily defeated? Opening include security check? Confirmation of locked at closing?
Interior Security Zones: Server Rooms File Rooms	Climate Control Unauthorized Access Unauthorized Information leaving area		
Computers (laptop)	Theft of computer Storage of computer (heat, cold) Theft of data	HD encryption (2 factor) User name / password access to network Locking time out Physically secure when unattended (cable/cabinet) Do not check as luggage Lock out of sight in the car /trunk Antivirus / spy ware / periodic firewall review	
Computer (network)	Theft of data Denial of Access	Rights management Acceptable use policy	

Security Plan Worksheet
Page 2 of _____

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*
Computers / Data	Access: Enforcement of Security Policy – Human Element	Determine user rights based on group needs, define the directory structure based on groups need, roles, responsibilities – allow them to access the areas they need Provide a written Proposal (Policy) for each type of group agreed to and signed by management and signed by employee As part of the policy, include users responsibility to report any anomalies with their system operation Define chain of responsibility within the policy Revisit the policy at least every 6 months and sign again Provide user training by group based on initial policy and ongoing 6 month refresh	

Security Plan Worksheet
Page 3 of _____

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*
Computers / Data	Access: Enforcement of Security Policy – Human Element	Provide warning banners users' on log on Conduct regular communication to all staff on security issues and confirm receipt of message Provide immediate communication to all staff on emergency situations - viruses, denial of service, spy ware, hacking	
	Enforcement of Security Policy – Infrastructure Element	Include Applied Access rights – Active Directory Provide Virus and patch updates – Push out from the server Provide Port Protection – Utility software Provide E-mail protection – virus scan, spy ware scan, integrity through signature software, spam protection Block undesirable services or sites through firewall, routers, monitoring logs	

Security Plan Worksheet
Page 4 of _____

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*
	Enforcement of Security Policy – Infrastructure Element	Protect the servers – use system logs, access logs, and application logs Detect intrusion through monitoring logs and warnings Provide VPN Security for remote users Improve dial-up security and preferably eliminate this access methodology Determine and provide solutions to the above	

Security Plan Worksheet
Page 5 of _____

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*
Personnel	Physical harm – Negligence Awareness of risks / threats	Emergency Procedures, dial 911 On the Job Training Quarterly Formal Training	

In Conclusion:

The *Information Security Policy – Tool Kit* presents an organized process of involving your entire organization in listing assets, describing vulnerabilities to those assets and offer mitigating controls to limit the likely hood of vulnerability exploitation. The result is a risk assessment, a security policy and a security plan.

The Internet forever changed the significance of proximity. Previously banks protected cash from theft; now the potential for identity theft may be as damaging as cash theft. During this time of revolutionary change, CSBS Best Practices hopes that the *Tool Kit* provided the opportunity for your agency to critically plan for security.

The *Security Policy Tool Kit* was structured to increase awareness, establish business practices, create routine due care and above all consider the issues of each agency in structuring agency policy. We hope you found the time and experience valuable.

CSBS Best Practices

Information Security Committee

SAMPLE PHYSICAL SECURITY POLICY:

Iowa Division of Banking

LAPTOP SECURITY POLICY

Last Updated: October 22, 2004

Purpose

This policy addresses the actions that must be taken by all Iowa Division of Banking (IDOB) personnel who have a state-issued laptop or the laptop of another employee.

Requirements

All laptops acquired for or on behalf of the IDOB shall be deemed state property. Each employee issued with a laptop is responsible for the security of that laptop, regardless of whether the laptop is used in the bank, the division headquarters, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport.

Security Precautions

Due to their size and portability, laptop computers are especially vulnerable to theft. Below are some guidelines IDOB staff are expected to adhere to:

- Do not leave a laptop in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave it in plain sight. If you must leave your laptop in a vehicle, the best place is in a locked trunk. If you do not have a trunk, cover it up and lock the doors.
- Be aware of the damage extreme temperature can cause to computers.
- Do not leave your laptop overnight at the bank unless the smartcard is removed and the laptop is locked in the bank's vault. Otherwise, take it with you.
- Never check a laptop as luggage at the airport. The Federal Aviation Administration has issued a warning about an increasingly common scam—stealing laptops from the conveyor belts of metal detectors. Wait for those ahead of you to pass through the metal detector before placing your laptop on the belt. Another airport scam to be aware of—one person will engage you in conversation or bump into you and their partner in crime will steal your laptop while you are distracted. Be alert.
- If you are leaving your work area, remove the smartcard from your computer.

- Do not let unaccompanied strangers wander around in your workplace. Offer assistance and deliver the person to their destination.

Precaution and common sense goes a long way in controlling your theft exposure.

General Information Management

Information, such as data, electronic mail, documents and software, are IDOB assets. In determining the value of an asset, consideration should be given not only to the sensitivity of the information, but also to the consequences of unauthorized disclosure, modification, destruction, or unavailability of the information. The value of these assets will determine the level of controls needed to provide adequate safeguards, backup and access controls.

- **Agency Records**. A "record" includes any information kept, held, filed, produced or reproduced by, with or for an agency in any form or media including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, forms, papers, images, photos, letters, microfilms, computer tapes or discs.
- **Password Protection**. Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the Comptroller and the employee's immediate supervisor. Employees must not post or share their personal passwords, and must develop secure passwords not likely to be guessed. Do not store your password on your machine and do not write your password down where it can be viewed by others. It is important to understand that once an unauthorized individual has your password, they have the ability to access the IDOB database.
- **Unattended Computers.** Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access. If smartcards are used, this would mean removal of the card when the machine is not in use. Laptops should never be transported with smartcards left in the machine.
- **Stolen Computer, Documents, or Media.** If an IDOB computer, documents, or media is stolen, the employee assigned responsibility for the computer should:
    - Notify the appropriate law enforcement agency and file a police report.
    - Immediately notify your Regional Manager, Comptroller, or Bureau Chief.
    - Make arrangements with the IDOB Comptroller for the return of your smartcard.
    - Provide a written summary describing details surrounding the theft. This could be the police report plus any other comments you feel are pertinent. Also, include details of information stored on the laptop.

Examination Information Management

- **Storage of Sensitive or Confidential Information.** All sensitive or confidential information should be retained only in an encrypted folder on your laptop.
- **Removal of Sensitive Information From the Laptop.** Once an exam report has been mailed by the IDOB to the bank, all members of the Region(s) involved with the exam will be notified by email the report has been mailed.
    - Upon receipt of the foregoing email, the EIC should check within two business days to see that all necessary examination-related information needed for future examinations are loaded onto the IDOB database. This would include GENESYS, ALERT, examination workpapers, and any electronic information provided by the banks including information provided in emails.
    - Within three days after receiving notice from the office the exam report has been finalized and mailed:
        - All examiners involved with the examination should remove all related examination information from their computer hard drives and any other storage devices including memory sticks. This would include, but not be limited to, GENESYS, ALERT, examination workpapers, and electronic information provided by the banks.
        - Any bank supplied examination materials or information should be destroyed, deleted, or returned to the bank.

Theft or Loss of Bank Customer Information

Once the IDOB becomes aware an IDOB computer containing bank customer information is stolen or lost the following events will occur:

- The Governor's Office will be notified by the Superintendent.
- The bank whose customer information has been compromised will be notified of the theft or loss.
- The primary federal regulator will be notified.
- Arrangements will be made with the bank and federal regulator for bank customer notification.
- IDOB legal counsel and senior management will prepare any needed press releases and procedures for handling calls from the press and bank customers.

It will be extremely important that all external communications be handled professionally. Such a loss has the potential to greatly harm the reputation and credibility of the IDOB. Liability to the division and individual examiner will potentially exist.

Violation of Policy

Disciplinary action, up to and including termination of employment, may be exercised in the event that these policies have not been followed. If an employee's laptop or smartcard is stolen or lost and the employee is deemed negligent, the employee will be held responsible for reimbursing the IDOB for replacement cost of the laptop or smartcard.

SAMPLE COMPUTER SECURITY POLICY:

DEFINITIONS

The following definitions were extracted from the State Administrative Manual ("SAM"), Section 4840.4.

CONFIDENTIAL INFORMATION – Information maintained by State agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. See SAM Section 4841.3.

INFORMATION ASSETS – (1) All categories of automated information, including (but not limited to) records, files, and data bases; and (2) information technology facilities, equipment (including personal computers systems), and software owned or leased by state agencies.

INFORMATION INTEGRITY – The condition in which information or programs are preserved for their intended purpose; including the accuracy and completeness of information systems and the data maintained within those systems.

INFORMATION SECURITY – The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.

PHYSICAL SECURITY – The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

PUBLIC INFORMATION -- Any information prepared, owned, used or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

SENSITIVE INFORMATION – Information maintained by state agencies that requires special precautions to protect it from unauthorized modification, or deletion. See SAM Section 4841.3. Sensitive information may be either public or confidential (as defined above).

IMPLEMENTATION – Practices and procedures used by Department employees to comply with this policy are as follows:

a. Do not disable or change the system password protection on notebook computers installed by the Information Systems Unit of the Department.

b. Do not write the password to the notebook computers on any paper material (business card, etc.), attach the password to the notebook computer, store the password on a file in the notebook computer or disclose the password to any unauthorized person(s).

c. Do not leave notebook computer(s), peripheral equipment(s) or electronic medium(s) (floppy disks, USB drives, CDs, etc.) unattended. The guidelines are as follows:

Department Licensee Site – If the above mentioned items (except for the electronic medium, which should be taken with you) will be left unattended for any length of time, the items will be placed in the carrying case and taken with you or placed in the licensee's vault. If the Licensee has provided a secure, lockable room, lock the room before leaving the room.

Department Employee's Home – If the above-mentioned items are at the Department employee's home, place the items in a safe, inconspicuous area.

Department Employee's Automobile – If the above-mentioned items are in the Department employee's car, place the items in the trunk or other concealed area of the automobile until the employee arrives at his/her home. Once at home, the employee must place the above mentioned items in his/her home. Do not expose the floppy diskettes to prolonged heat exposure, as it will destroy the floppy diskettes.

Traveling on State Business – If the above-mentioned items are in the Department employee's hotel room, place the items in a safe, inconspicuous area or with the hotel's concierge. At the airport, train station, etc., always hold onto the above mentioned items. Watch your notebook at all times as it enters and exits the airport x-ray machine. Thieves have been working in pairs to create a diversion at the x-ray area of airports, allowing one thief to walk off with the notebook as it exits the x-ray machine, while the other holds up the x-ray machine line by having to re-enter the scanning device numerous times. Do not set the above mentioned items down as most thieves can spot portable computer carrying cases and will steal the computer from you in seconds.

d. Do not disable or stop the AntiVirus program that is automatically started when the notebook computers are turned on.

e. Always run a virus scan on any diskettes or USB thumb drive that you place in the notebook computers.

f. Never stop the antivirus or patch management programs from updating your machine with the virus definition files or with the system security updates and patches.

g. Do not leave diskette(s), USB thumb drive(s) or any security token(s) in the notebook computer carrying case(s). These items must be kept in a separate location to prevent loss of information in the event the notebook computer is stolen and from unauthorized access when the notebook computer is locked in the Department licensee's vault.

h. To ensure the further protection of Department information assets, at the direction of the Executive Committee or the Financial Institutions Manager or Financial Institutions Supervisor Committees, a password or encryption may be required on documents using the appropriate software application password or encryption feature. If this password protection is required, the password will not be written on paper materials or disclosed to unauthorized person(s).

i. The notebook computer's hard drive should only be used to store the current examination. All previous examinations should be transferred to the appropriate network share drive at the completion of the examination.

j. Any electronic media used to transfer examination information from one notebook computer to another should be immediately erased at the completion of the transfer.

k. Electronic media received from the financial institution which contains confidential personal customer information should be destroyed after transferring the information to a secure network drive or into the Genesys or Alert program. All other media should be safely stored with the examination work papers.

l. No unauthorized software will be installed in the notebook computers.

m. The hardware and software configuration set by the Department's Information Systems Unit will not be changed on the notebook.

n. No copies of Department software or equipment configurations will be provided or disclosed to unauthorized person(s).

o. No Department notebook computer, peripheral equipment or electronic medium(s) will be made available to unauthorized person(s) for his/her/their use.

p. No unauthorized peripheral equipment will be installed or connected to the notebook computer; and no unauthorized personal computer will be connected to Department peripheral equipment.

q. All Department information assets printed at the office or at a Department licensee's site must be shredded before discarding. If the Department licensee's site does not have a paper shredder, all Department information assets printed at a Department licensee's site

must be brought back to the office and properly shredded before discarding.

r. Do not write the Department dial-in telephone number(s) or remote access password on any paper material (business card, etc.) or disclose the telephone number(s) or password to any unauthorized person(s).

s. Do not write the Department's Outook Web Access URL or your username and password on any paper material (business card, etc.) or disclose the telephone number(s) or password to any unauthorized person(s).

t. Do not write the Department's Intranet Address or the username and password on any paper material (business card, etc.) or disclose the telephone number(s) or password to any unauthorized person(s).

u. All repair(s) to notebook computers and peripheral equipment will be performed by an authorized, contracted service provider of the Department.

COMPLIANCE -- All employees of the Department shall comply with this policy and associated information security directives. Information systems must not be installed or used in such a manner as to provide the opportunity to create unauthorized links to other systems, bypass authentication mechanisms, circumvent data access control procedures, or otherwise jeopardize the security of any or all components within the Department network.

All violations of the Department's security policies and/or procedures are subject to disciplinary action. The specific disciplinary action to be rendered will be dependent upon the nature of the violation, the impact of the violation on the Department's information assets and related facilities, etc.

SECURITY INCIDENT REPORTING -- All actual or suspected instances of information asset or equipment theft and abuse, as well as potential threats (e.g. hackers, computer viruses, fire) or obvious control weaknesses affecting security, must be reported immediately to the local system administrator or to the Information Systems Unit Manager.

REFERENCES:

(The Best Practices group does not control the following web sites; thus while the content was relevant during the development of the Security Kit, we do not guarantee the site content.)

CSBS:
Contingency Planning:
http://www.csbs.org/tech/techbulletinboard/Contingency%20Planning/contingency-planning.htm

FFIEC:
Information Security:
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

ISACA:
General IT Audit Guidance:
http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=6693

The Institute of Internal Auditors
General Awareness:
http://www.theiia.org/

Password Crackers:
www.openwall.com/john/

Physical Security – Locks
http://security.org/dial-80/links.htm

National Institute of Standards and Technology
http://www.itl.nist.gov/

WWW security
http://www.w3.org/Security/Faq/www-security-faq.html

FDIC:
www.fdic.gov

Federal Reserve
www.federalreserve.gov

RISK ASSESSMENT

To be completed by: _____

Page ____ of _____

Define the scope of security by clarifying the asset, the threat to the asset and mitigating measures.

Asset / Resource	Threat	Mitigating Measure

Blank Risk Assessment work sheet page.

Security Plan Worksheet
Page ______ of ________

Asset	*Vulnerabilities / Threats / Risks*	*Procedures/ Controls*	*People or log that confirms the control*