STATE OF HAWAI'I
INFORMATION PRIVACY AND SECURITY COUNCIL

Category	**Security**	Title	**Security of Laptops, Removable Data Storage Devices, and Communication Devices**
Document:	**IPSC2009-01**	Revision:	**2009.08.28-01**
Posted URL:	http://ipsc.hawaii.gov		
Status	Adopted	Revised on:	August 28, 2009
Authority:	**State of Hawai'i IPSC**	Exceptions:	Temporary Allowed
Applicability	☒State Government Agencies ☒All ..... Guideline ☐Excluding: None ..... Not Applicable ☐Including: None ..... Not Applicable ☒State Funded Entities ..... Guideline ☒Other: County Government Agencies & Attached ..... Guideline		

I. PURPOSE

Laptops, portable storage devices, smart phones, personal digital assistants (PDAs) and other mobile technologies and communication devices are being used with increasing frequency to perform and support the daily operations of all Counties and State of Hawaii departments and agencies. The convenience of using such devices contribute to the increased usage of these mobile technologies in State and County agencies and their compact size make them attractive targets for theft. The purpose of this document is to provide basic guidelines for all State and County agencies for protection of sensitive information in these mobile computing environments as described in Act 10 of the State Legislative Special Session in 2008.

II. SCOPE

These guidelines are provided to all State and County government agency IT managers whose employees have been assigned use of or have access to any agency-owned electronic mobile device or use non-agency-owned electronic mobile devices to access and/or store agency information (if permitted by the agency).

This guideline meets only the requirements imposed by the State of Hawaii. Agencies/Departments that work with federal information of a confidential or sensitive nature must ALSO ensure laptops and other electronic mobile devices are in compliance with all requirements and policies at the federal level.

III. TERMS AND DEFINITIONS

Personal Information – As defined in Act 135 and Act 136, Session Laws of Hawaii 2006, an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number;
2. Driver's license number or Hawaii identification card number; or
3. Account number: credit or debit card number, access code, or password that would permit access to an individual's financial account. (Note: Includes pCard/credit cards issued to employees for agency purchase purposes)

Sensitive Information – Any type of information such that the loss, misuse, or unauthorized access to or modification of could adversely affect the Counties and State of Hawaii departments and agencies. Personal information as defined above are considered to be a subset of "Sensitive Information". Examples of sensitive information includes information protected by other regulations such as HIPAA and FERPA.

Encryption – Transformation of information into a form that cannot be read or interpreted by others without knowledge of how it was transformed. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

IV. POLICY

All State and County government agency employees are responsible for the safekeeping of any agency-issued electronic mobile device assigned to them and for securing all sensitive information stored on and transmitted via any electronic mobile devices and environments.

All State and County government agency employees must provide immediate notification to their respective agencies and/or supervisors following the loss of any agency-owned electronic mobile device or the loss or compromise of any sensitive information.

Appropriate and timely action must be taken if Sensitive and/or Personal Information is contained on the lost or stolen electronic mobile device in accordance with the Agency's Policies and Procedures.

V. STANDARDS

Laptop computers, net book computers, and other mobile computing devices:

Use of laptop computers, net book computers, and any other similar mobile computing devices are increasing in proliferation in County and State agencies allowing for its employees to access email and other institutional applications from remote, off-site locations. While increasing productivity, use of these devices without taking the proper security precautions also increase the risk of data compromise or loss. Basic security guidelines for mobile computing devices are:

1. All mobile computing devices should adhere to basic computing security standards such as:
    a. System should be configured with user accounts with strong passwords.
    b. Apply regularly scheduled operating system and application security updates.
    c. Install and maintain anti-virus and anti-spyware software.
    d. Backup the mobile computing device on regular basis. Appropriate security precautions should be taken to protect the backup files.
2. Use of Encryption:
    a. Sensitive information stored on mobile devices must be encrypted.
3. Physical security:
    a. Use physical locking devices such as anti-theft cables or motion detection sensors.
    b. Do not leave laptops unattended for even a short while.
    c. Do not leave mobile computer devices locked in the trunk of a car.
    d. Do not leave laptops unattended and exposed in hotel rooms.

Additional measures that may provide additional protection but are not yet considered industry best practices include:

a. Install laptop recovery software such as LoJack or ZTrace.
b. Use biometric authentication in addition to user accounts and strong passwords.
c. “Self-destruction” of data on stolen laptop – lost data destruction.

Removable Storage Devices (CD/DVDs, USB drives, memory sticks, etc.)

As with laptop computers, the cost and size of removable storage devices (CD/DVDs, USB drives, memory sticks, external hard drives, etc.) are decreasing. These devices offer a convenient method to store and transport data. But if proper security guidelines are not followed when storing sensitive information on these devices, the risk of data loss or compromise greatly increases. The following guidelines should be used whenever possible:

1. Minimize use of removable storage devices for storage of sensitive information.
2. Securely erase sensitive information as soon as it is no longer needed.
3. Encrypt sensitive information.
4. Physical security:
    a. Do not store removable storage devices with the mobile computing device.
    b. Secure the removable storage device in a locked storage unit when not in use.
5. Establish policies to address sensitive information stored on removable storage devices that are tailored specifically to each agency’s needs.

Communication Devices used for remote access to agency applications:

Cell phone, smart phones, PDAs, and other mobile communication devices have become convenient and valuable tools aiding in the mobility of the workforce. These small and relatively inexpensive devices are being used with increasing frequency to access County and State agencies' email and application servers. Email and files containing sensitive information may be stored on these devices. While these devices increase productivity, they pose an increased risk factor when sensitive information is stored on these devices without proper precautions. . The following guidelines should be used whenever possible:

1. Activate the password protection on the mobile device.
2. Activate the auto-lock feature on the device and set it to auto-lock if the device is not used for 5 minutes.
3. If available, enable auto-destruction of data on the device if the password is entered incorrectly 10 times or utilize the remote wipe capabilities.
4. Securely erase all information on the device before disposal or recycling.
5. Encrypt sensitive information stored on communications devices.

Transmission of Sensitive Information:

Use secure protocols and processes such as (but not limited to) encryption, HTTPS, SFTP, SSH, SSL and VPNs whenever sensitive information is transmitted over public or unsecured/unknown private networks. Users should particularly be advised of the insecurity of public hotspots and the importance of security protocols when these networks must be used.

When transmitted by email, sensitive information should be protected at the appropriate level in accordance to the sensitivity of the information being transmitted. As an example, if social security numbers are transmitted, encrypted email or password-protected zip files should be used.

Policies on Protection of Sensitive Information:

All State and County agencies should develop policies governing use and storage of sensitive information. Policies should define governance, definition, roles and responsibilities, use, transmission, storage and destruction of sensitive information as applicable for each agency.

Policies and Procedure on Loss of Any Electronic Mobile Device:

All State and County agencies should develop policies governing the loss of any electronic mobile device as applicable for each agency. Policies and Procedures should include reporting of the loss, an audit for any sensitive information contained on the device, and required timeframe for reporting.

Security Awareness Training for End Users:

All State and County agencies should educate their user communities about their roles and responsibilities in the protection of sensitive information. Users should also sign agency-specific confidentiality agreements to indicate their understanding of their roles and responsibilities.

VI. MONITORING

All State and County government agencies have the right to monitor, review, audit, and/or disclose any and all aspects of use of the agency's technology resources in accordance with the applicable policies of the agency.

VII. ENFORCEMENT

Violations of State and County government agency policies will be governed by policies specific to each agency and applicable laws & regulations.

VIII. REFERENCES AND ATTACHMENTS

State Information:

Computer and Network Resources Acceptable Use Policy:
http://www4.hawaii.gov/dags/icsd/ppmo/Stds_Web_Pages/IT0800/IT0800s0.htm

DHRD Acceptable Usage of Information Technology Resources:
http://www.higov.net/portal/Members/dhrd/StateWideSupp/DHRDPnP/

University of Hawaii Information:

E2.214: Security and Protection of Sensitive Information:
http://www.hawaii.edu/apis/ep/e2/e2214.pdf
UH Form 92: UH General Confidentiality Notice:
http://www.hawaii.edu/ohr/docs/forms/uh92.pdf
Best Practices for Laptop Users:
http://www.hawaii.edu/askus/927
IT Security at UH:
http://www.hawaii.edu/askus/729

NIST Information:

NIST documents can be reviewed at:
http://csrc.nist.gov/publications/PubsSPs.html

SP 800-111: Guide to Storage Encryption Techniques for End User Devices
SP 800-114: User's Guide to Securing External Devices for Telework and Remote Access
SP 800-121: Guide to Bluetooth Security
SP 800-122 : Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

SP 800-124: Guidelines on Cell Phone and PDA Security

General Information:

Protecting Portable Devices: Physical Security:
http://www.us-cert.gov/cas/tips/ST04-017.html
Good Security Habits:
http://www.us-cert.gov/cas/tips/ST04-003.html
Safeguarding Your Data:
http://www.us-cert.gov/cas/tips/ST06-008.html
Cyber Security Tips:
http://www.us-cert.gov/cas/tips/
Effectively Erasing Files:
http://www.us-cert.gov/cas/tips/ST05-011.html
Laptop Security:
http://www.onguardonline.gov/topics/laptop-security.aspx
9 Ways to Increase the Security of Your Laptop While on the Road:
http://www.microsoft.com/atwork/stayconnected/laptopsecurity.mspx

IX. COMMENTS AND SUGGESTIONS

Comments, recommendations, proposals, or suggestions regarding the contents of this document may be sent via email to:

IPSC@hawaii.gov

or in writing to:

Information Privacy and Security Council
c/o Information and Communication Services Division
1151 Punchbowl Street, Room B10
Honolulu, HI 96813

X. REVISION HISTORY

Creation Date:	Date Last Updated	Date last reviewed
August 28, 2009	August 28, 2009	August 28, 2009

Revision History		
Revision date	**Revision**	**Author**
Aug 28, 2009	2009.08.28-01 First Issue	Information Privacy & Security Council

Russ K. Saito, Chairperson
Information Privacy and Security Council

8/28/09
Date