South Carolina Department of Parks, Recreation and Tourism **DEPARTMENT POLICY**	Policy Number 702.7	Page Number 1
	Effective Date: April 27, 2009	
	Supersedes:	Dated:

Subject:

IDENTITY THEFT PROTECTION POLICY

PURPOSE AND SCOPE:

This policy is adopted to help protect full time employees, temporary employees, customers, contractors and consultants from damages related to the loss or misuse of personal identifying information and other sensitive information.

DEFINITIONS:

"Personal Identifying Information" consists of a person's first name or initial combined with their last name and unencrypted or unredacted data including the person's social security number or driver's license number or financial account number(includes credit card, debit card and security code) or other numbers or information that would allow access to the person's financial accounts.

"Other Sensitive Information" includes but is not limited to the following items whether stored in electronic or printed format: business identification number, employer identification number, paychecks, pay stubs, medical information such as doctor names and claims, insurance claims, prescription, any related personal medical information, and other personal information such as date of birth, address, phone number, or maiden name.

"Security Breach" is the unauthorized access to, and acquisition of, items containing personal identifying information and the illegal use of the personal identifying information has occurred or is likely to occur.

SECURITY MEASURES FOR HARDCOPY RECORDS:

Each employee, contractor and consultant performing work for SCPRT will comply with the following practices:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with personal identifying and/or other sensitive information will be locked when not in use.

2. Storage rooms containing documents with personal indentifying and/or other sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing personal identifying and/or other sensitive information when not in use.

APPROVED _____ DIRECTOR DATE April 27, 2009

(Rev. 1-94)

4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

SECURITY MEASURES FOR ELECTRONIC RECORDS:

Each employee, contractor and consultant performing work for SCPRT will comply with the following practices:

1. Internally, transmittal of personal identifying and/or other sensitive information by using approved agency e-mail should be limited. Personal identifying and/or other sensitive information will be stored in agency public folders in Outlook, the agency's email system. Access to this information should be restricted to only designated SCPRT employees.

The following disclaimer must be present in the body of the email:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom/which it was originally addressed. Any use by others is strictly prohibited."

2. Any personal identifying and/or other sensitive information transmitted externally must be encrypted (SSL or SSH) and only transmitted to approved recipients.

3. Personal identifying and/or other sensitive information should only reside on the personal network drive (H :/) of the owner of the documents, or on the AS400.

4. Personal identifying and/or other sensitive information **will not be copied to the personal hard drive (C :/) of user's PC, the agency shared network drive (X :/) or shared Office drive**.

5. Personal identifying and/or other sensitive information **will not be copied to external media, including USB drives, CDs or DVDs.**

6. Personal identifying and/or other sensitive information **will not be copied to SCPRT employees' or contractor's laptop computers.**

South Carolina Department of Parks, Recreation and Tourism **DEPARTMENT POLICY**	Policy Number 702.7	Page Number 3
	Effective Date: April 27, 2009	
	Supersedes:	Dated:

Subject:

IDENTITY THEFT PROTECTION POLICY

SCPRT will limit the potential of the release of personal identifying information or sensitive information by utilizing internal forms/documents that do not include unnecessary personal identifying or sensitive information. New forms created will also limit the amount of personal identifying or sensitive information provided.

DISPOSAL OF HARDCOPY RECORDS:

Reasonable measures will be implemented to ensure the proper disposal of information and prevent the unauthorized access to and use of the personal identifying and/or other sensitive information. When hardcopy documents containing personal identifying and/or other sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded. **However, agency records may only be destroyed in accordance with the agency's records retention policy.**

The employee using the personal identifying and/or other sensitive information in a hard copy format will be responsible for properly disposing of or securing the information.

DISPOSAL OF ELECTRONIC RECORDS:

The Director of Technology Services will verify that all personal identifying and/ or other sensitive information is removed from computer hard drives and backup tapes and are sanitized in accordance with the Budget and Control Board standards and policies. Agency records may only be destroyed in accordance with the agency's records retention policy.

SECURITY BREACH:

In the event of a security breach, the employee, customer, contractor or consultant who first becomes aware of the breach will immediately notify the director of the agency. When SCPRT discovers or is notified of a security breach within the agency, the person or persons whose personal identifying information has been exposed will be notified immediately by telephone, fax, or electronic means. Once a person has been notified, a subsequent "security breach notification letter" will be sent within two business days from discovery of the breach informing the victim of the expected date of the breach, explaining steps taken by the agency to prevent further harm, advising whether law enforcement or the Department of Consumer Affairs was notified. In the event more than 1000 persons at one time have been affected, the Department of Consumer Affairs and the three major credit reporting agencies will be contacted.

APPROVED _____ DIRECTOR DATE April 27, 2009

(Rev. 1-94)