### Revision Log

<table>
<thead>
<tr>
<th>Pages Affected</th>
<th>Description of Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global</strong></td>
<td>Added Section 5.3.5 Personally Owned Electronic Equipment (POEE) Use. Added Attachment 8.1 and 8.2.</td>
</tr>
<tr>
<td>3</td>
<td>Section 5.2 added the 4th and 10th bullet.</td>
</tr>
<tr>
<td>4</td>
<td>Section 5.2 rewrite of the 4th bullet. 5th bullet and sub bullets under added for unclassified mobile device locations</td>
</tr>
<tr>
<td>5</td>
<td>Section 5.2 added 4th bullet: Connect any government owned equipment (e.g., desktops, laptops, instruments, etc.) to the Guest Wireless Network [SRSGuestNet Wi-Fi]. Approved centrally managed government iOS devices are exempt from this requirement.</td>
</tr>
<tr>
<td>8-11</td>
<td>Sections 5.2.8, 5.2.10 and 5.2.11 and 5.3.2 total rewrite of the sections.</td>
</tr>
</tbody>
</table>
1.0 PURPOSE [S/RID 1, 2, 3, 4, 5]

This appendix provides the Code of Conduct that has been developed to define appropriate activities associated with the use of computing systems, devices, and resources, both classified and unclassified, under the cognizance of the Savannah River Site (SRS), and to eliminate inappropriate computer use that may expose SRS to risks, which includes compromise of information, networks and services, and legal issues.

2.0 SCOPE

The provisions of this procedure apply to the Performing Entities at the SRS and to any other site tenant(s) that have consented by written agreement (e.g., Functional Service Agreements) to comply with this procedure, and to subcontractors performing work for the Performing Entities or tenant(s) when required by subcontract or applicable law.

3.0 DEFINITIONS AND ABBREVIATIONS

General definitions and abbreviations applicable to this procedure are provided in Manual 10Q, Appendix 601, Definitions and Abbreviations.

4.0 RESPONSIBILITIES

All users of federal systems, devices and networks are responsible for reading, understanding, and signing/acknowledging this Cyber Security Code of Conduct. Users are expected to consult Manual 10Q for clarification of requirements and any specific organizational policies.

5.0 CODE OF CONDUCT

5.1 Monitoring and Expectation of Privacy

Federal computer systems, devices, and networks implemented for SRS use are the property of the United States Government.

Users (authorized and unauthorized) have no expectation of privacy. Any and all use of such systems, devices, and networks may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized SRS, Department of Energy (DOE), and law enforcement agencies, as well as authorized officials of other agencies.

By using SRS computing resources, the user consents to such interception, monitoring, recording, copying, auditing, inspecting, and disclosure at the discretion of authorized personnel.

Unauthorized or improper use of federal resources may result in administrative disciplinary action, up to and including termination and civil and criminal penalties.

Non-federal computer systems that have been approved for processing SRS information are subject to the same monitoring and inspection requirements as stated for federal computer systems.
5.2 General Use

The following requirements are associated with common activities for users of federal computing resources.

Users shall:

- Use government computer resources for official business and in accordance with the terms of this Code of Conduct and the requirements from the applicable organizational policy.
- Only utilize unclassified government resources for personal use in accordance with their specific organizational ethics guidance; employees may only make limited use of government resources for personal purposes and such personal use must involve de minimis (insignificant) additional expense to the government.
- Comply with the requirements of Manual 10Q, as applicable.
- Comply with the requirements of “SRS Mobile Device Acknowledgment”. See Attachment 8.2.
- Secure information systems before leaving them unattended (e.g., log out, session lock, door lock, etc.).
- Report any violation of this Code of Conduct, including any known, unprotected Controlled Unclassified Information (CUI) or classified information, to the line manager/Subcontract Technical Representative (STR).
- Comply with copyright, trade secret, patent and other intellectual property laws and regulations, as well as similar laws or regulations governing the use of software.
- Present true identification and authentication credentials.
- Comply with SRS’ sexual harassment and workplace violence prevention policies by not using any government resources to actively engage in acquisition, transmission, or the display of material that is in violation of policy.
- Ensure computers taken off-site have an approved security configuration [e.g., Cyber Security Configuration Management Team (CSCMT)].
- Contact the Enterprise Cyber Security Operations (ECSO) if any unusual or suspicious activity is noticed regarding the computer system or connection to a SRS network including:
  - A resource used by SRS that is hosting malicious content (e.g., systems or web sites infected with malware).
  - A web site that appears to be redirecting users to sites with prohibited or malicious content.
5.2 General Use, (cont.)

Users shall not:

- Reconfigure, circumvent, or disable any protective/security measures for any SRS computer systems, devices, or networks (e.g. authentication, firewall, anti-virus, configuration settings, SRS Virtual Private Network (VPN) client)
- Transmit or store site data on External Information Systems (EIS) (e.g., cloud storage, home computers, personal mobile devices, etc.) without prior approval via the Release of Information (ROI) process
- Effect security breaches and/or disruptions of any network communications, including use of any resource as a staging ground to gain unauthorized access to other systems
- Knowingly introduce malicious programs into the network or computing systems (e.g., viruses, worms, Trojan horses, unauthorized “hacking software” etc.)
- Introduce computing devices with wireless communications and/or activated camera or microphone into an NNSA Limited Area (LA) or higher without prior authorization from the Officially Designated Federal Security Authority (ODFSA)
- Introduce unclassified mobile devices in the following locations:
  - SRS Sensitive Compartmented Information Facility (SCIF)
  - Special Access Program (SAP) Facility
  - TEMPEST Areas
  - Classified Conference Rooms
  - Material Access Areas
  - Vault or Vault Type Rooms
  - Rooms containing secure (classified) telephony (STE, STU, vIPER, etc.) when this equipment is in use
  - Areas approved for routine Top Secret discussions
  - Rooms with COMSEC equipment not in a safe
  - Rooms where classified computer processing is in progress
- Create or forward “chain letters,” mass mailings, “Ponzi” or other “pyramid” schemes of any type
- Create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials
- Create, download, view, store, copy, transmit, or retransmit materials that support gambling, illegal weapons, terrorist operations, or criminal activities
- Create, download, view, store, copy, or transmit materials in the conduct or furtherance of any type of illegal activity
5.2 General Use, (cont.)

- Engage in social networking, including instant messaging and chat on government devices. Approved centrally managed enterprise government iOS devices are exempt from this requirement.
- Allow use of government computer resources by anyone without proper access credentials.
- Install controlled software on government resources without prior approval; for examples of controlled software, refer to the ECSO Computer Security Web site.
- Connect any government owned equipment (e.g., desktops, laptops, instruments, etc.) to the Guest Wireless Network (SRSGuestNet Wi-Fi). Approved centrally managed government iOS devices are exempt from this requirement.

Several specific types of information can be sent to your home email accounts. These types include:

- Messages from Employee Communications that relate to employee benefits.
- Safety-related information.
- Class work that has been approved under the Tuition Reimbursement Program.
- Messages related to DOE or company sponsored activities.

5.2.1 Physical Protections

Users shall not release computer systems, software or other associated media from SRS without sanitization.

Prior to releasing information, users shall obtain Release of Information (ROI) approval as identified in Manual 1B, Procedure 105, Release of Information. Scientific and Technical Information (STI) is a category of External Release Information. The requirements and procedure for the capture of STI, including the definition of STI, are contained in Manual 1B, Procedure 3.25, Capture, Management and Disposition of Scientific and Technical Information.

5.2.2 Data and Information Protection

Users shall:

- Comply with Manual 7Q, Procedures 404, Identification of Classified Matter, and 406, Identification and Protection of Controlled Unclassified Information (CUI), that ensure media is adequately protected according to its classification level and sensitivity level.
- Only process information on computers approved for that sensitivity level of information.
- Obtain organizational Information Security approval prior to transmitting or storing site data on External Information Systems (EIS) (e.g., cloud storage, sending government email home, etc.)
5.2.2 Data and Information Protection, (cont.)

- Apply the least privilege principle by ensuring their rights and privileges are relevant to the assigned duties and areas of responsibilities
- Know the classification level and sensitivity level of the information or contact a Derivative Classifier/Reviewing Official (DC/RO) for guidance if unsure of the data classification prior to processing, storing, or transmitting
- CUI information over unprotected public networks (e.g., internet, etc.) must be transmitted in accordance with Manual 7Q, Procedure 406, Identification and Protection of Controlled Unclassified Information
- Ensure CUI, which includes Personally Identifiable Information (PII), is not posted, shared or divulged on any open internet or social media site
- Exercise due diligence when allowed access to PII in maintaining its normal security protection measures (i.e., copying PII to a test environment without maintaining the same level of security measures is not acceptable)
- Report, upon discovery, all suspected or actual loss, compromise, or theft of protected Personally Identifiable Information (PII), to line management/STR and/or to the Savannah River Site Operations Center (SRSOC), 725-1911, as applicable to your organizational policies (Manual 7Q, Procedure 315)
- Use only SRS approved online storage or file sharing services (e.g., Proteus) where required for conducting government business with outside entities.

Users shall not execute any form of unauthorized network monitoring that has potential to intercept data.

Users or their line manager/STR, shall notify the information owner/steward of any change in status that will affect their access (e.g., organization, clearance, employment status).

5.2.3 Passwords

Users shall:

- Protect passwords minimally at the same level of protection required for the data
- Comply with the password rules published on the ECSO Cyber Security Web site
- Change their password/credential immediately, or ensure that the associated account is disabled by the responsible system administrator, when a compromise of personally-assigned password or credential is suspected or known.

Users shall not:

- Share personally-assigned credentials (i.e., personal pin codes and passwords, private encryption keys)
- Auto-enter or auto-save passwords within any application [e.g., log-in scripts, Internet Explorer (IE) dialogs].
5.2.4 Connections

Users shall connect their centrally managed computers to SRSnet at least monthly to receive security patches, software updates, and antivirus signatures.

Users shall not connect EIS to SRS-operated systems (e.g., desktops, laptops, printers, scanners, and networks).

- A method exists for connecting EIS to the SRS network using approved/established methods (e.g., the SRS managed Citrix client access).
- An approved method also exists for non-SRS network connection only if used explicitly to establish a network connection to SRSnet via the Virtual Private Network Broadband (VPNBB); network activities on the SRS computer must then be only through the VPNBB connection.

5.2.5 Foreign National Access

Users shall not grant any computer resource access to Foreign Nationals without appropriate DOE authorization as outlined in DOE O 142.3A, Unclassified Foreign Visits and Assignments Program, and included in Manual 7Q, Procedure 510, Control of Visits – Foreign Nationals, and Form OSR 10-304, Unclassified Foreign Visit/Assignment Request Form.

5.3 Remote Access and Mobile Device Use

The following requirements are associated with additional common activities for remote and mobile device users:

- Mobile hotspots shall not be connected to SRSnet.

Mobile hotspots are not to be used or established in or near Limited Areas and higher. If a mobile hotspot is used in a general site or property protection area, the hotspot name must not match the naming convention utilized by SRS or appear that the hotspot is an approved SRS hotspot or SRS access point. For example, a mobile hotspot should not be named SRSnet, GuestNet, SRS Guest, etc.

5.3.1 Physical Protections for Offsite Use

Users shall:

- Ensure that adequate measures are taken to protect SRS mobile devices from unauthorized access, alteration, modification, disclosure, transmission, destruction, or theft as prescribed in applicable SRS site-wide procedures to include:
  - Protection while in use by maintaining physical control and not allowing unauthorized access
  - Protection during storage by the use of physical locks.
5.3.1 Physical Protections for Offsite Use, (cont.)

- Contact the SRS Operations Center at (803) 725-1911 immediately if a computing resource is lost or stolen from off-site (e.g., missing laptop, etc.).

Users shall not check government owned/leased mobile computing resources in baggage at an airport, train depot, taxi, or hotel valet, etc.

5.3.2 Data and Information Protection

Users shall:

- Minimize the use of CUI (UCNI, OUO, and/or other sensitive information as identified in Manual 7Q, Procedure 406) data on mobile devices to the level required to perform the job function.

- Ensure that all computing resources, including mobile devices, provide protection of CUI data by utilizing FIPS 140-2 encryption prior to removing the device from an SRS controlled area or facility.

- Assume that government owned mobile devices may be in the area and must be proactive when a classified discussion is about to begin and ask for the removal of mobile devices from the immediate area.

- Assume that government owned mobile devices may be in the area and must be proactive when a CUI discussion is about to begin and ask for all recording to cease during the conversation.

Users shall not:

- Discuss, store, or transmit classified information on government mobile devices.

- Discuss Unclassified Controlled Nuclear Information (UNCI), on government owned mobile devices.

- Store CUI on any non-government computing resource without prior DOE approval.

- Use the audio recorder except for Business Use Only reasons, nor take photographs, or video with a government owned mobile device where the topic may be considered classified or Controlled Unclassified Information (CUI). See Manual 7Q, Procedure 406 for types of CUI at SRS.
5.3.3 Connections Established

Users shall:

- Use only the DOE authorized points of entry (e.g., the managed VPNBB or Citrix services) for accessing SRS systems remotely.
- Obtain approval, where required, from Export Control, Counterintelligence, and ECSO before transporting SRS mobile media computing resources to foreign countries.
  
  - The M&O centrally managed Citrix implementation for use with personal computers to connect to SRSnet may be used within the Contiguous United States (CONUS) (i.e., the contiguous 48 states, not including Alaska and Hawaii) without additional approvals; however, additional review and approval is required for any connection outside of the Contiguous United States specifically for the RSA SecurID token, using form OSR 10-328, Request for Temporary Export of Equipment for International Travel.
  
  - The M&O centrally managed Virtual Private Network for broadband (VPNBB) connection of government computers to SRSnet is allowed only for CONUS use.

Users shall not establish direct simultaneous connections from government-owned computers or devices (e.g., desktops, laptops, tablets) to SRSnet and any other network (e.g., guest Wi-Fi).

5.3.4 Government iOS (iPad/iPhone) Device Use

**NOTE**

This section applies to government owned iOS (iPad, iPhone) devices. See Manual 10Q, Procedure 300, Unclassified Cyber Security Program Requirements, for policy on personally-owned electronic equipment (POEE).

Users shall only use government owned iOS (iPad/iPhone) devices for unclassified purposes.

Users shall not introduce government owned iOS (iPad/iPhone) devices without prior authorization from the Officially Designed Federal Security Authority (ODFSA) in the following locations:

- SRS Sensitive Compartmented Information Facility (SCIF)
- Special Access Program (SAP) Facility
- TEMPEST Areas
- Classified Conference Rooms
- Material Access Areas
5.3.4 **Government iOS (iPad/iPhone) Device Use**, (cont.)

- Vault or Vault Type Rooms
- Rooms containing secure (classified) telephony (STE, STU, vIPER, etc.) when this equipment is in use
- Areas approved for routine Top Secret discussions
- Rooms with COMSEC equipment not in a safe
- Rooms where classified computer processing is in progress
- NNSA facilities and/or locations within a LA or higher level of security area.

Mobile device users shall consult the Manual 7Q, Procedure 312, *Prohibited and Controlled Articles*, for the requirements that outline the general Technical Security requirements.

Users of government owned iOS (iPad/iPhone) devices shall comply with these additional requirements:

- Users may download Apple Store apps to the device
- Users acknowledge that all devices are subject to management and configuration policies as defined in site mobile device management tool and are subject to remote wipe if lost or device appears compromised
- Users may connect the device to their personally owned computer only for backup, synchronization, patching and charging
- Users may connect government iPads or iPhones to a personal hotspot to accomplish Citrix connectivity
- Users may connect to the Guest Wireless Network. See Attachment 8.1 for the Guest Wireless (SRSGuestNet Wi-Fi) User Rules of Usage
- Users shall not connect to SRS government equipment (e.g., desktops, laptops, monitors, etc.). This includes charging the device by connecting them to government equipment
- Users shall not enable AirDrop
- Users shall not enable Family Sharing
- Users shall not enable Share My Location
- Users shall not enter any PII in the HealthKit Medical ID section
- Users shall not store any information in Apple Pay
- Users shall not use or program auto answer, or audible or one digit speed dialing while in a LA or higher level of security area
- Users shall not use for entertainment streaming media purposes while in a LA or higher level of security area. Streaming for business purposes is authorized.
5.3.5 Personally Owned Electronic Equipment (POEE) Use

**NOTE**


Users may connect Personally Owned Electronic Equipment (POEE) to the Guest Wireless Network. See attachment 8.1 for the Guest Wireless (SRSGuestNet Wi-Fi) User Rules of Usage.

Users shall not introduce Personally Owned Electronic Equipment (POEE) within Limited Areas or higher without prior approval from the ODFSA.

Personal Fitness Monitoring Devices (PFMD) are exempt from this requirement within EM LAs.

PFMDs are prohibited in NNSA LAs or higher level of security area.

Smart watches are not exempt from this requirement and are not permitted in LAs or higher level of security area.

Users shall not connect personally owned iPad, iPhone, PFMD, smartphones, or other tablets to SRS government equipment (e.g., desktops, laptops, monitors, etc.). This includes charging the device by connecting them to government equipment.

5.4 Privileged Use

The following requirements apply additionally to all who use increased rights, permissions or privileges to allow the modification of security settings; this includes those assigned on a permanent basis (e.g., database roles granted, domain administrator, UNIX sudo privileges, application and service accounts, etc.) or a temporary basis (e.g., Help Desk temporary addition for special purpose, such as additional application installations, emergency accounts, etc.).

Privileged Users shall:

- Follow any additional requirements within relevant security plans and organizational procedures including configuration management, contingency planning, vulnerability and patch management handling, incident response handling
- Document, investigate, and report to ECSO all suspected cyber security related events in accordance with applicable site and organizational policies and procedures
- Submit to the Information System Security Officer (ISSO) any potential security significant change for review and subsequent Information System Security Manager (ISSM) determination prior to implementation
5.4 Privileged Use, (cont.)

- Use their elevated/privileged access only when performing official duties that require the access; a general user account shall be used for duties where an administrative account is not a requirement (e.g., internet web browsing does not require an administrative access; users with temporary administrative assignments must not access the Internet while the regular account is a member of local administrator group)
- Access only the data for which authorized and a need to know exists
- Grant requests for access to another end user’s e-mail or files (archived or otherwise) from a documented request that includes a proper business justification (e.g., termination, extended absence, etc.) from all of the respective and appropriate management of the parties involved
- Ensure adequate protection of shared privileged account accesses (e.g., adhere to passwords management rules, do not share with anyone unauthorized for access, etc.).

5.5 Acknowledgment

I acknowledge that I have read the foregoing Cyber Security Code of Conduct, that I fully understand its contents, and that I agree to comply with all requirements therein. Furthermore, I understand and acknowledge that I may request and review any and all documents cited in the Cyber Security Code of Conduct prior to acknowledging this Code of Conduct.

If I am unbadged, I give permission to SRS to conduct appropriate personal investigative screening to grant computer access.

____________________________________ _____________________________
User Name (Print First, MI, Last)

Company/Organization/Dept/Division

____________________________ ______________________ _________ ___ (Y/N)
User Signature   User ID (If available)  Date  US
Citizen?

____________________________________ ____________________ ___________
COR/STR/Host (Please Print)   User ID  Date
6.0 REFERENCES

5B, Human Resources Manual

5B, 1-4, General Human Resources Program

7Q, Security Manual

7Q, 312, Prohibited and Controlled Articles

7Q, 404, Identification of Classified Matter

7Q, 406, Identification and Protection of Controlled Unclassified Information

7Q, 510, Control of Visits – Foreign Nationals

10Q, Cyber Security Manual

DOE-Savannah River Operations Office (SROO) Policy 08-07

DOE Document Review Sheet SR-60

DOE O 142.3A, Unclassified Foreign Visits and Assignments Program

Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules

NNSA Policy Letter NAP-14.1-D, Baseline Cyber Security Program

Office of the Under Secretary of Energy, Program Cyber Security Plan (PCSP) version 2.0

[S/RID 1 (Standards/Requirement Identification Document)], DOE O 206.1, Department of Energy Privacy Program

[S/RID 2] DOE O 200.1A, Information Technology Management


[S/RID 4] DOE N 205.1, Unclassified Cyber Security Program (LW only)

[S/RID 5] DOE O 205.1B, Department of Energy Cyber Security Program (M&O only)

WSI SRS Team-SRS Standard Procedure 1-2253, Cyber Security Program

7.0 RECORDS

Records generated as a result of implementing this procedure are maintained in accordance with Manual 1B, Procedure 3.31, Records Management.
7.1 Forms

OSR 14-357LN  Request for Information Review and Release

OSR 10-328  Request for Temporary Export of Equipment for International Travel

OSR 10-304  Unclassified Foreign Visit/Assignment Request Form

8.0 ATTACHMENTS

Attachment 8.1  Guest Wireless Network (SRSGuestNet Wi-Fi ) User Rules of Usage

Attachment 8.2  SRS Mobile Device Acknowledgement
ATTACHMENT 8.1

Guest Wireless Network (SRSGuestNet Wi-Fi) User Rules of Usage
Page 1 of 1

The Guest Wireless Network is a Department of Energy (DOE) computer system. All data contained within DOE computer systems are owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OR REASONABLE EXPECTATION OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO ANY ACTIVITY RELATED TO AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, OR DISCLOSURE OF COMPUTER ACTIVITY.

The Guest Wireless Network is provided as a convenience, and performance / availability will be on a best-effort basis.

The Guest Wireless Network may be used by site visitors, on-site vendors, and site personnel. The Guest Wireless Network is not protected and all users of the guest network are liable and responsible for the data and information they transmit over the guest wireless network.

SRS retains the right to deny access to the Guest Wireless Network at its sole discretion at any time or for any reason whatsoever.

Personnel may connect government-issued iphones and ipads to the Guest Wireless Network. SRS government-provided laptop and desktop computers are prohibited from connecting to the Guest Wireless Network unless specifically authorized through a DOE-SR approved Risk Assessment.

Personnel may also connect non-government devices to the Guest Wireless Network. These devices are the sole responsibility of the owner and no Help Desk services will be provided to assist individuals with connecting such devices.

The Guest Wireless Network may not be used for gambling purposes and may not be used to view, record, or disseminate sexually explicit or sexually oriented material.

Contact your Ethics Office or Workforce Services representative with questions about acceptable use and/or rules concerning guest wireless network.

Last Updated: November 18, 2015
SRS Government owned mobile devices such as Cellular Phones, Smart Devices and Tablet Computers, are allowed in the General Site and Property Protection Areas (PPAs). Effective January 2016, SRS U.S. Government owned mobile devices are allowed within the SRS Limited Area (LA) or higher level security area within Environmental Management (EM) facilities, except where signs are posted prohibiting any mobile device.

**Government mobile devices are NOT permitted within NNSA LA or higher level facilities or locations.**

Employees who have been issued a U.S. Government owned mobile device are required to sign this acknowledgement prior to the introduction of the Government owned mobile device into an LA or higher level security area.

******************************************************************************

1) I ______________________ (print user name) understand that my Government owned mobile device is a long range wireless device which will transmit information outside of the secure perimeter and SRS boundary, care should be exercised for what is being discussed when using my Government owned mobile device.

2) I will only use my Government owned mobile device for unclassified purposes. I will not use the Government owned mobile device to discuss, store, or transmit classified information. I will not discuss UCNI on my Government owned mobile device.

3) I will not introduce my Government owned mobile device into any of the locations (listed below) that are located within SRS security areas, to include:
   - Sensitive Compartmented Information Facilities (SCIFs)
   - Special Access Program (SAP) Facilities SRS
   - TEMPEST Areas
   - Classified Conference Rooms
   - Material Access Areas (MAAs)
   - Vault or Vault Type Rooms (VTRs)
   - Rooms containing secure (classified) telephony [STE, STU, vIPER, etc.] when this equipment is in use
   - Areas approved for routine Top Secret discussions
   - Rooms with COMSEC equipment not in a safe
   - Rooms where Classified computer processing is in progress.
4) I will follow all postings and signs that prohibit electronic devices from designated locations.

5) I understand that when a classified discussion is about to begin, that the speaker must announce that the discussion is going classified and all devices must be removed from the immediate area.

6) I understand that mobile device audio recording and camera use on-site is allowed for unclassified government business only. I will ensure a security review is conducted by the appropriate information security personnel if I have any doubt regarding the sensitivity or classification of audio recordings, photographs, or video taken with a U.S. Government owned mobile device.

7) I will not have my Smart Device/Cellular Telephone unattended, programmed for auto answer, or audible or one digit speed dialing while in a LA or higher level security area.

8) I understand that before entering any area or facility onsite, it is my responsibility to verify that the U.S. Government owned mobile device is authorized.

9) I will not use my mobile device for entertainment streaming media purposes while in the LA or higher. Streaming for government business purposes is authorized.

10) Failure to comply with the requirements listed in this acknowledgement will result in the immediate retrieval of the mobile device and the initiation of an Incident of Security Concern.

If my U.S. Government Mobile Device is ever a lost, or stolen or suspected compromise of information associated with this device, I will immediately contact the Savannah River Site Operations Center (SRSOC) at 803-725-1911 and my supervisor for instructions.

Signature: __________________________ User ID: ___________ Date: ____________________

This device is subject to security audit at any time.