1. **PURPOSE:** The purpose of the Information Security Incident Management Plan is to define the School’s procedures for handling information security incidents, including contact information for personnel with responsibility for responding to the incident, plans to contain an incident, and procedures on how to restore information, if necessary. This procedure supplements the University’s Incident Management Policy.

2. **SCOPE:** This procedure applies to all School of Government employees including temporary employees, and those computers owned by the School of Government (SOG) covered in the Computer Lifecycle Replacement Plan (CLRP) or purchased through the School. Those computers not covered by the CLRP or purchased by the School will not be managed by the Departmental Incident Response Team (DIRT) and the employee should contact the ITRC directly. It specifically addresses those systems where storage of sensitive data may occur or to divisions where there is a high likelihood of sensitive data access as identified in the School of Government Annual Sensitive Data Survey.

   It is assumed that all School employees have read and are adhering to the University of North Carolina at Chapel Hill sensitive data policies (UNC-CH) as outlined in the Information Security Policies Summary (http://help.unc.edu/CCM3_020433).

   A security incident includes any incident that is known to or has the potential to negatively impact the confidentiality, integrity, or availability of UNC-CH’s information. This can range from the loss of a laptop, the virus infection of an end-user workstation, or a major intrusion by a hacker.

   All School of Government employees shall report actual or perceived security incidents in the following manner:

   a. Call the School of Government Helpdesk at 962-5487 or submit a Remedy Ticket from the SOG IT Help page

   b. Contact the School of Government Information Security Liaison at 962-8197 or email at allen@sog.unc.edu

   c. If no contact or response, email or call the contact the School of Government Information Security Liaison Backup at 966-4460 or email at balfour@sog.unc.edu

   d. If you believe university-owned sensitive data is at risk alert the Information Security Office by calling the Information Technology Response Center at 919-962-HELP or
submitting a Remedy ticket for assignment to the ITS-Security Remedy group. It is essential that you submit the ticket as “critical” and provide a phone number where you can be reached.

e. Users who have a security incident with their personal computer or smartphone may choose to contact the Information Technology Response Center at 919-962-HELP. If the personal computer or smartphone hosts university-owned sensitive data or uses the same passwords as university owned systems, the user must follow the actions outlined in Step d above. The School of Government’s Departmental Incident Response Team (DIRT) does not manage personally owned devices.

   i. Personal computers, those not owned by the SOG, are not supported by the School’s Information Technology Division and will not be managed by the Departmental Incident Response Team (DIRT). Personal computers should not be used for storing or accessing sensitive data pertaining to work at the University of North Carolina at Chapel Hill.

   ii. Smartphones, those not owned by the SOG, are not supported by the School’s Information Technology Division and will not be managed by the DIRT. The IT division can provide documentation to access SOG Email and campus wireless networks with smartphones. Mobile devices that work with sensitive data should connect via the UNC-Secure wireless network SSID rather than UNC-1 or Tarheel SSIDs. Users may also contact 919-962-HELP for assistance with their smartphone.

3. GENERAL: The department will respond to information security incidents by initiating a Departmental Incident Response Team (DIRT). The DIRT will be comprised of:

   - The School of Government Information Security Liaisons and any necessary technical support personnel
   - The School of Government Assistant Dean for IT
   - The System Administrator for the affected information system
   - The person or person(s) capable of identifying the types of data residing on the affected system/s
   - A representative from the ITS Security Office (ISO)

When there is an identifiable risk to sensitive information, the School’s Information Technology Division will issue a critical ticket to the ITS-Security Remedy group prior to performing any system scanning or cleanup actions. They will also log in the ticket, the date and time when notification from the end user occurred and any known IP or MAC addresses for the system.

Incidents can happen any day of the week and any time of the day and ISO or DIRT may disable network access for systems at any time to ensure protection of sensitive information. If administrators believe that sensitive information is being actively exfiltrated to unauthorized parties, it may be appropriate to disable network access to the system to ensure protection of sensitive information. Otherwise, no action should be taken until an ISO incident handler is consulted.
4. PROCEDURES: Preparation Stage of Incident Management

The School of Government will take the following measures to anticipate the most likely types of information security incidents in our environment and prepare for them. This work only applies to computers owned and managed by the School of Government.

a. Annual Sensitive Data Survey – An annual survey will be administered at the School to help identify and evaluate the sensitive data environment. The results of this survey will be used by the Departmental Incident Response Team (DIRT) to identify where proactive management will need to occur.

b. Inventory – An inventory of systems identified in the survey as storing sensitive data or are critical to the university/school mission (sensitive/critical) will be performed to ensure efficient incident management.

c. Vulnerability Management – The School of Government schedules weekly Qualys vulnerability scans and Symantec virus scans for computers identified in the survey as storing sensitive data. They will also ensure automatic updates are enabled where possible.

d. Communication Protocol
   i. All contact information for the DIRT should be readily available prior to the onset of an incident. A copy will be maintained at the School’s Helpdesk in case an incident results in loss of access to such contact information.
   
   ii. Where required, external breach notification requirements will be cataloged and appropriate contact information be available prior to the onset of an incident (i.e. federally funded research contract with contractual breach notification clauses). The School’s Business Office will keep the catalog of records for this information and provide copies to the DIRT. Breach notifications are implemented by the department under the direction of the Office of University Counsel and with consulting support from ISO.
   
   iii. The DIRT will provide guidance to the ISO regarding how they would like ISO to contact them or their delegates when incidents arise. The ISO uses the Cujo database as the primary source for contact information.

e. Testing – The School of Government will test their incident management procedures in advance of a real information security incident and again on a regular basis thereafter.

f. Incident Response, Containment and Eradication Phases
   i. Identification – The first step in incident management is to identify and confirm the incident. When an incident occurs, care will be taken to understand the scope of the incident, the likelihood of proliferation to additional systems, and the types of data at risk. Incidents will be classified according to incident levels specified below.

<table>
<thead>
<tr>
<th>Incident Level</th>
<th>Examples</th>
<th>Investigation Type</th>
</tr>
</thead>
</table>


| Level 1          | • Violation of UNC sensitive data Policies  
|                 | • Violation Acceptable Use Policy  
|                 | • Violation of UNC Password Policy  
|                 | • Virus infection of end-user desktops  
|                 | • Basic investigation of an incident  
|                 | • Remediation advice for an incident  
|                 | • Device isolation, if necessary  
| Level 2         | A suspected incident involving sensitive information stored on a system or device owned or managed by the University or hosting University sensitive information  
|                 | Investigation of an incident potentially involving unauthorized access of sensitive information or a mission-critical system  
| Level 3         | An incident involving sensitive information on a University-owned or managed system or device or a system hosting such University information where the initial investigation indicates a likelihood that sensitive information was successfully accessed by an intruder  
|                 | • Investigation of a likely or confirmed breach of a system processing or storing sensitive information or a mission-critical system  
|                 | • Investigation of information technology relevant issues performed in support of criminal or civil cases, as well as University internal investigations  

**Table 1: Incident Levels**

ii. **Do Not Destroy Evidence of the Unauthorized Activity** – When incidents occur resulting in possible risk to sensitive data, no action including scans of the system will be taken until an incident responder from the ISO is consulted. The system should not be shut down. Malware should not be deleted. Unauthorized accounts should not be deleted. Incident responders may need the above information to help them determine the nature and extent of the incident.

If it appears that sensitive data is actively being accessed by unauthorized parties, system administrators may disable access to terminate the unauthorized access but should not take additional steps until directed to do so by an incident handler. If the system administrator should decide to terminate access by unauthorized parties, s/he should take the minimum action necessary to disable the unauthorized access until communications with an ISO incident handler can be initiated. An example of the latter might include disabling of the network access by removing the network cable.

iii. **How to Reach ISO** – If sensitive data is believed to be in danger as a result of an information security incident, a member of the DIRT will call the Information Technology Response Center at 919-962-HELP and ask that a critical Remedy ticket be created for the ITS-Security group or will directly submit a critical Remedy ticket for assignment to the ITS-Security Remedy group. If it is a non-covered machine the employee should contact the Information Technology Response Center at 919-962-HELP as outlined above.
iv. **Collaboration to Contain and Eradicate the Unauthorized Activity** – Once the incident has been reported, ISO will work with a member of the DIRT to address the problem. We will anticipate the following requests from the ISO:

a) **What types and amounts of sensitive data may be in danger?** The results of the sensitive data survey will be used to guide this answer.

b) **What business critical services would be impacted by isolation of an affected host that performs critical business functions?**

g. **System Rebuild** – Intrusions usually result in complex alterations of systems and an inability to “clean” a system may occur. After an intrusion, systems will need to be rebuilt, if feasible.

h. **Lessons Learned**

i. After every incident, the ISO and the DIRT will be available for a “lessons learned” collaboration meeting. The purpose of the meeting is to jointly do a post evaluation on the root causes of the incident and together consider actions that could prevent recurrence.

ii. The ISO will not share School of Government-specific information identified during this meeting unless expressly allowed to do so by the School or unless ISO is advised to do so by Office of University Counsel. The ISO will give the School of Government an opportunity to respond and/or edit an incident report prior to it being closed with the ISO and the Office of University Counsel.

iii. In a timely fashion, the ISO will communicate information regarding incidents that could lead to additional compromises.

5. **APPROVAL:**

________________________________________________________________________
(Department Head or Designate)

________________________________________________________________________
(Director of ITS Security)