On-Site Inspection Guideline

Please refer to the On-Site Inspection Procedures before using this Guideline.

Organization Name: ____________________________

Address: ______________________________________

Date and time of inspection: ______________________

The data base(s) that the licensee possess(es) is/are:

__________________________________________________________________________

The type of license is: ____________________________

Person interviewed: ____________________________

Name of inspector: ______________________________

Inform the Person Interviewed

This is an unannounced inspection as you agreed to in Section IV (G) of your license to have access to a data base containing individually identifiable information. Our main goal in conducting these inspections is to make sure licensees are in compliance with the requirements of the statutes, as outlined in the security procedures and the license. If we find a licensee out of compliance, our objective is to provide advice and assistance to achieve compliance.
On-Site Inspection Guideline

Please confirm the names of the Senior Official, Principal Project Officer and project staff with the interviewee. The names for “as listed in License” may be obtained from the licensee’s file.

Name of the Senior Official?

As listed in License

As stated in Inspection

What is the name of the Principal Project Officer (PPO)?

As listed in License

As stated in Inspection

What are the names of other people who have access to the data?

<table>
<thead>
<tr>
<th>As listed in License</th>
<th>As stated in Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Who is responsible for day-to-day security of the data?

As listed in Security Plan

As stated in Inspection

______________  _____________
**On-Site Inspection Guideline**

<table>
<thead>
<tr>
<th>LICENSE PROCEDURES</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is there on file:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. a copy of the License?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. signed Affidavits? (if applicable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. any Amendment (Memorandum) that alters the original License? (if applicable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. a copy of the Security Plan?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Have a copy of the <em>Security Procedures</em> and License been given to all members of the project staff?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. It is important that the staff fully understand the security procedures and license agreement. Have they read and do they understand the security procedures and license and understand penalties towards any violations?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Has any legal, investigatory, or other demand for disclosure of subject data been received?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If yes, has the demand been reported to the Agency?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Has any breach or suspected breach of security or any disclosure of subject data to unauthorized parties or agencies been discovered?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If yes, has the (suspected) breach been reported to the Agency?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PHYSICAL HANDLING, STORAGE, AND TRANSPORTATION

6. Where are the data stored when not in use? (All restricted-use materials must be securely stored when not in use. The materials are to be properly catalogued and kept under lock and key, preferably in a fire proof cabinet. Data shall not be in a computer facility library unless all who have access to the library media hold affidavits.)

7. How are the data handled? (The security procedures must limit potential access to the data and restrict access to only those with an executed affidavit, or otherwise authorized by the Agency. Computer personnel who mount tapes or load data on the system must also hold affidavits.)

8. Are data used at the licensed site only?  
   If no, where else are they used? (Data are not to be removed from the licensed site. This includes using data at home or providing it to a sub-contractor to use off-site.)

9. Are the data transported from the facility?  
   If yes, how are they transported? (Data must be carried by a person with an executed affidavit or by a bonded courier and in a sealed envelope or secured container or sent by certified mail.)
On-Site Inspection Guideline

10. Have any copies been made of the subject data?  
   If yes, was it of the entire database? *(This is allowed only once.)*  
      Only a subset of the database?  
      Where are those copies now? *(Copies should be stored as securely as the original database.)*

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Who has access to those copies? *(They can be made available only to individuals holding affidavits.)*

11. What type of monitoring procedures are being used when the project staff access the database? *(Inspector(s) should check the security features to ensure that all procedures have been properly followed. Also, when checking the materials, make sure that the 9-track tapes, CD-ROMs, or diskettes have a restricted data notification label. The notification should state the database’s restricted use and the expiration date of the license.)*

12. Have any print copies containing individually identifiable information been made?  
    Where are those copies now? *(Copies should be stored as securely as the original database.)*

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13. Are all printouts, tabulations, and reports edited for any possible disclosures of subject data?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
COMPUTER SECURITY REQUIREMENTS

14. What type of computer hardware arrangement is used to access the data?

_____ Standalone Computer - Continue to question 15
_____ Standalone LAN - Go to question 16 on page K-7
_____ Safe Workgroup within a LAN - Go to question 17 on page K-8

15. **Standalone Computer**

   a. Is room/area access limited? __ __

   b. Are passwords used? *(Password protection must always be used on portable computers. On nonportable computers, passwords are one means that may be used to shut down or lock up computers.)*

      If yes, are passwords unique, 6-8 characters with one non-alphanumeric? __ __

   c. If passwords are used, are they changed at least every three months? __ __

   d. Is there notification (e.g., a warning screen) on each computer? __ __

   e. Is there read-only access? __ __

   f. Have all connections to other computers been shut down? __ __

   g. Is the computer/room physically locked when the authorized user is out of the room, or has automatic “shutdown” been enabled? __ __

   h. Are there any routine backups of restricted-use data? __ __

   i. If passwords are used, are they changed when staff changes? __ __

   j. At the end of the project or if the hard disk needs repair, has the hard drive been overwritten? __ __

*Go to question 18 on page K-10.*
16. **Standalone Local Area Network (LAN)**

16.1 Requirements for Standalone Computer (that also apply to Standalone LAN)

   a. Is room/area access limited? [Yes / No]

   b. Are passwords unique, 6-8 characters with one non-alphanumeric? [Yes / No]

   c. Are passwords changed at least every three months? [Yes / No]

   d. Is there notification (e.g., a warning screen) on each computer? [Yes / No]

   e. Is there read-only access? [Yes / No]

   f. Have all connections to another LAN or external computer been shut down? [Yes / No]

   g. Is the computer/room physically locked when the authorized user is out of the room, or has automatic “shutdown” been enabled? [Yes / No]

   h. Are there any routine backups of restricted-use data? [Yes / No]

   i. When an employee leaves the project— is his or her password/access rights to the restricted-use data removed? [Yes / No]

   j. At the end of the project or if the hard disk needs repair, has the hard drive been overwritten? [Yes / No]

16.2 Additional Requirements for Standalone LAN

   a. Is LAN room locked when unattended by sworn individual(s)? [Yes / No]

   b. Is access to server console restricted (e.g., password)? [Yes / No]

   c. (For Standalone LAN PCs that are in non-adjoining rooms)
      Is the password encrypted by the PC/workstation software (instead of by the server software) so it cannot be intercepted in plain text form on its way to the server? [Yes / No]

*Go to question 18 on page K-10.*
### On-Site Inspection Guideline

#### 17. SAFE WORKGROUP within a LAN

**17.1 Requirements for Standalone Computer (that also apply to Safe Workgroup)**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Is room/area access limited?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Are passwords unique, 6-8 characters with one non-alphanumeric?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Are passwords changed at least every three months?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Is there notification (e.g., a warning screen) on each computer?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Is there read-only access?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. (This question is not applicable to Safe Workgroup.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Is the computer/room physically locked when the authorized user is out of the room, or has automatic “shutdown” been enabled?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Are there any routine backups of restricted-use data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. When an employee leaves the project—is his or her password/access rights to the restricted-use data removed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j. At the end of the project or if the hard disk needs repair, has the hard drive been overwritten?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**17.2 Requirements for Standalone LAN (that also apply to Safe Workgroup)**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Is LAN room locked when unattended by sworn individual(s)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Is access to server console restricted (e.g., password)?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**17.3 Additional Requirements for SAFE WORKGROUP within a LAN**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Is access to subject data restricted to sworn workgroup members only who can login from workgroup PCs only?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Are workgroup PCs on-site, in restricted access areas, and identified by network interface card (NIC) number at login?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
c. Is the password encrypted by the PC/workstation software (instead of by the server software) so it cannot be intercepted in plain text form on its way to the server?  

   Yes  No

---

d. Are there access controls for subject data directories and files that limit access by:
   (1) group or access control list to sworn workgroup members only?  
   (2) read-only rights?  
   (3) attributes (e.g., delete inhibit)?

   Yes  No

---

e. Are the following prohibited on workgroup server/PCS with subject-data access:
   (1) TCP/IP server software?  
   (2) remote-control software?  
   (3) peer-to-peer connectivity?

   Yes  No

---

f. Does the system audit capability record the name, user ID, time in/out, and NIC number of every access to the subject data base and all failed access attempts?  

   Yes  No

---

g. Does the PPO review a printed copy of the audit log monthly, initial it, and maintain a file of monthly audit logs for a year?  

   Yes  No

---

h. Are the server console and printer(s) password-protected and located within the limited access room/area?  

   Yes  No

---

i. Have additional security measures been implemented, as determined by the licensee? *(Any additional security measures must be annotated in the Security Plan.)*

   Yes  No

   If yes, what are they?

   __________________________________________________________
   __________________________________________________________
   __________________________________________________________
   __________________________________________________________
On-Site Inspection Guideline

Inform the Person Interviewed

We remind you that licensees are required to provide the Agency a copy of each publication containing information based on subject data. Additionally, if a publication or other release of research results could raise reasonable questions regarding disclosure of individually identifiable information contained in subject data, copies of the proposed publication or release must be provided to the Agency before that disclosure is made.

18. Finally, have you had any problems using the data?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

19. Within the confines of the law, is there any way you could suggest to make the licensing process any easier?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
On-Site Inspection Guideline

To be completed after inspection.

Additional Comments from the Inspector. Please provide any other relevant information that you found during the inspection.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Summary of licensee’s compliance. If you found anything out of compliance, please explain what was out of compliance at the licensee site and provide possible reasons for these violations. This section will be used by the Data Security Program to decide what penalties to impose on the licensee.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Signature of Inspector ________________ Date ________________