Quarterly Compliance Checklist

HMIS Partner Agency Name:				Technical Administrator Name:
Q1 – Jan. □	Q2 - April □	Q3 - July □	Q4 – Oct. □	Date:

Workstation Security Standards

This Compliance Certification Checklist is to be completed quarterly by the Partner Agency Technical Administrator for the HMIS Partner Agency named above. Every agency workstation used for HMIS data collection, data entry or reporting must be evaluated. Attach additional copies of any page of this checklist as needed. Any compliance issues identified must be resolved within 30-days. Upon completion, a copy of this checklist should be forwarded to the HMIS Lead Agency (David Webster, dwebster@countyofsb.org). This original checklist should be readily available on file at the HMIS Partner Agency for 7 years.

For the purpose of this section, authorized persons will be considered only those individuals who have completed HMIS Security and Privacy training within the past 12 months.

1. A Privacy Notice is visibly posted at the HMIS workstation. If multiple HMIS workstations are located in the same room, a single Privacy Notice may be posted if it is easily visible from each HMIS workstation.
2. HMIS workstation computer is in a secure location that is not accessible to clients, casual volunteers, or visitors.
3. HMIS workstation computer is password protected and locked when not in use.
4. Documents printed from HMIS are sent to a printer in a secure location that is not accessible to clients, casual volunteers, or visitors.
5. Non-authorized persons are unable to see the HMIS workstation computer monitor.
6. HMIS workstation computer has antivirus software with current virus definitions (within the last 24 hours) and a full system scan within the past week.
7. HMIS workstation has and uses a hardware or software firewall.
8. If HMIS is accessed via wireless internet, the wireless internet network must be secure (password required to connect).
9. Unencrypted Protected Personal Information (PPI) has not been electronically stored or transmitted in any fashion (hard drive, flash drive, email, etc.).
10. Hard copies of PPI (client files, intake forms, printed reports, etc.) are stored in a secure location.
11. Password is kept physically secure.
12. HMIS workstation computer does not store or "memorize" HMIS related passwords.

#	Workstation Location & End User Name(s)	1	2	3	4	5	6	7	8	9	10	11	12	Notes/Comments
1														
2														
3														
4														
5														
6														

7														
8														
9														
10														

	Workstation security compliance issues identified	**Steps taken to resolve workstation security compliance issue**

Technical Administrator Certifications

(Initials) I have verified that:

________ All agency End Users are using the most current version of the HMIS Consent Form for Release of Information.

________ All agency End Users have signed the End User Agreement, and I maintain a file of all of those signed agreements.

________ All agency End Users are exclusively accessing HMIS from a workstation subject to these quarterly security audits.

________ All agency End Users have completed Privacy and Security training within the past 12 months.

________ All agency End Users require access to HMIS to complete their assigned duties.

________ The owner, authorized user, model, and serial number of each laptop used to access HMIS is written down and on file.

____ ________

Partner Agency Technical Administrator Signature *Date*

____ ________

Executive Director (or other empowered officer) Signature *Date*