Nebraska State Purchasing Bureau
Request for Proposal for Licensure Information System (LIS)
RFP 6249 Z1

Exhibit 14 – GCOM Security Plan Template

Prepared By:

GCOM

GCOM Albany (Corporate Headquarters)
24 Madison Avenue Extension, Albany, NY 12203

Table of Contents

Table of Tables

Security Plan Section Template and Questionnaire

1. Application / System Identification

1.1 System Identification

1.1.1 System Name / Title

Enter the System Name and acronym given to the general support system or application.

1.1.2 Responsible Organization

In this section, list the organization that owns and is responsible for the data in the application. The responsible organization owns the system, the data it contains, and controls the use of the data. Include phone numbers, physical locations, and addresses.

1.1.3 Information Contact(s)

Specify the program owner, program manager and the system manager to contact for further information regarding the security plan and the system. Include their address, telephone numbers, and e-mail. List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. The contacts given should be identified as the system owner, program manager, and system manager. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

1.1.4 Assignment of Security Responsibility

List the Information System Security Officer (ISSO), or other person(s) responsible for the security of the system, including their address and phone number. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system. Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system.

1.1.5 Authorizing Official

The authorizing official is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The authorizing official has the following responsibilities related to system security plans:

- Approves system security plans,
- Authorizes operation of an information system,

- Issues an interim authorization to operate the information system under specific terms and conditions,

or

- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

1.2 Operational Status

Indicate whether the system is operational, under development (or acquisition), or undergoing a major modification. Include date of operation, expected implementation, or completion of modification.

1.3 General Description / Purpose

Present a brief description (one to three paragraphs) of the function and purpose of the system. If the system is a major application describe and provide a data flow diagram. If the system is a general support system, list all applications supported by the general support system. Specify if the application(s) is or is not a major application and include unique name / identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations pertaining to this system, whether they are internal or external to the system owner’s organization, and a general description of the type of information and processing provided.

1.3.1 Mission Criticality

The System’s Mission Criticality must be documented here.

1.4 System Environment

Provide a brief (one to three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented; The software resides on an open network used by the general public or with overseas access;
- The application is processed at a facility outside of the organization's control; or
- The general support mainframe has dial-up lines.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

Specify any system components that are essential to its operation, but that are not included within the scope of the plan, and the reason that this is so (i.e., covered under another plan, etc.).

1.5 System Interconnection / Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to affect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

1.6 Sensitivity Of Information Handled

This section provides a description of the types of information handled by the system, an analysis of the sensitivity of the information stored within, processed by, or transmitted by a system and appropriate background investigation required for access.

The description will provide information to a variety of users, including:

- Analysts / programmers who will use it to help design appropriate security controls
- Internal and external auditors evaluating system security measures
- Managers making decisions about the reasonableness of security countermeasures and,
- Users accessing the system including:
    - system administrators,
    - database administrators, and / or
    - application support staff members completing the appropriate background investigation forms.

1.7 Applicable Laws Or Regulations Affecting The System

List any laws, regulations, or policies that establish specific requirements for confidentiality of data / information in this specific application. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information).

2 Management Controls

2.1 Risk Assessment

Describe the risk assessment methodology used to identify the threats and vulnerabilities of the application / system.

List the group that conducted the assessment, and the date(s) the review was conducted.

If there is no application / system risk assessment, include a milestone date (month and year) for completion of the assessment.

2.2 Review of Security Controls

List any independent security reviews conducted on the application / system.

Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

2.3 Rules of Behavior

A set of rules of behavior must be established in writing for each application / system. The rules of behavior should be made available to every user prior to the user receiving access to the application / system, with a signature page to acknowledge receipt. The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the application / system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other application / systems.

2.4 Planning for Security in the Life Cycle

In this section, determine which phase(s) of the life cycle the application/system, or parts of the application / system, are in.

- Initiation
- Development / Acquisition
- Implementation
- Operation / Maintenance
- Disposal

Identify how security has been handled during each of the listed applicable life cycle phases.

3 Operational Controls

3.1 Personnel Security

Table 1 Personnel Security

Considerations	Yes	No
Have all positions been reviewed for sensitivity level?	☒	□
Have individuals received background screenings appropriate for the position to which they are assigned?	☒	□
Is user access restricted to the minimum necessary to perform the job?	☒	□
Is there a process for requesting, establishing, issuing, and closing user accounts?	☒	□
Are critical functions divided among different individuals (separation of duties)?	☒	□

- Discuss mechanisms in place for holding users responsible for their actions.
- Discuss friendly and unfriendly termination procedures.

3.2 Physical and Environmental Protection

Discuss the physical protection in the area where application / system processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, fire safety, plumbing leaks, HVAC failure, etc.).

3.3 Production, Input / Output Controls

Provide a synopsis of the procedures that support the operations of the application / system. Describe the controls used for the marking, processing, storage, and disposal of input and output information and media, as well as the labeling and distribution procedures for information and media. The controls used to monitor the installation of application / system software updates should also be listed.

3.4 Continuity of Operations (Contingency Plan/Disaster Recovery)

Briefly describe the procedures (contingency plan) that would be followed to ensure the application / system continues to be processed if the supporting IT application / system were unavailable. Include descriptions for the following:

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
- Location of stored backups and generations of backups
- Are tested contingency / disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Coverage of backup procedures, e.g., what is being backed up?

If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan may be attached as an appendix.

3.5 Application / System Hardware and Software Maintenance Controls

Table 2 Application / System Hardware and Software Maintenance Controls

Considerations	Yes	No	N/A
Are there restrictions / controls on those who perform hardware and software maintenance and repair activities?	☒	☐	☐
Are there special procedures for performance of emergency repair and maintenance?	☒	☐	☐
Are there procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?	☒	☐	☐
Are there procedures used for controlling remote maintenance services where diagnostic procedures or maintenance are performed through telecommunications arrangements?	☒	☐	☐
Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?	☒	☐	☐
Was the application / system software developed in-house or under contract?	☒	☐	☐
Is the application / system software a copyrighted commercial off-the-shelf product or shareware?	☒	☐	☐
Has the software been properly licensed, and have enough copies been purchased for the application / system?	☐	☐	☒
Are there organizational policies against illegal use of copyrighted software and shareware?	☒	☐	☐
Is there version control that allows association of application / system components to the appropriate application / system version?	☒	☐	☐
Are all changes to the application / system software or application / system components documented?	☒	☐	☐
Are there impact analyses to determine the effect of proposed changes on existing security control to include the required training for both technical and user communities associated with the change in hardware / software?	☒	☐	☐
Are there change identification, approval, and documentation procedures?	☒	☐	☐
Are there procedures for ensuring contingency plans and other associated documentation are updated to reflect application / system changes?	☒	☐	☐
Does the change control process require that all changes to the application / system software be tested and approved before being put into	☒	☐	☐

Considerations	Yes	No	N/A
production?			
Are there procedures for testing and / or approving system components (operating system, other system, utility, applications) prior to promotion to production?	☒	□	□
Is test data live data or made-up data?	□	□	□
Do test plans trace back to the original security requirements?	□	□	□
Are test results documented?	□	□	□

3.6 Data Integrity / Validation Controls

Table 3 Data Integrity / Validation Controls

Considerations	Yes	No	N/A
Is virus detection and elimination software installed?	☒	□	☒
If so, are there procedures for updating virus signature files, automatic and / or manual virus scans, and virus eradication and reporting?	☒	□	□
Are reconciliation routines used by the application / system, i.e., checksums, hash totals, record counts?	□	☒	□
Are integrity verification programs used by the application / system to look for evidence of data tampering, errors, and omissions?	□	☒	□
Is an intrusion detection tool installed to monitor the application / system?	☒	□	□
Are procedures in place to handle and close out security incidents?	□	☒	□
Are other network security software packages used?	□	□	☒
Is application / system performance monitoring used to analyze performance logs in real time to look for availability problems, including active attacks, and application / system and network slowdowns and crashes?	□	☒	□
Is penetration testing performed on the application/system?	□	☒	□
If so, what procedures are in place to ensure that tests are conducted appropriately?	□	□	☒
Is message authentication used in the application / system to ensure that the sender of a message is known and that the message has not been altered during transmission?	□	□	☒

3.7 Documentation

Documentation includes descriptions of the hardware and software, policies, procedures, and approvals related to automated information security in the application / system. Documentation should also include descriptions of user and operator procedures, and backup and contingency activities.

3.8 Security Awareness and Training

Describe the type and frequency of application / system specific training provided to employees and contractor personnel (workshops, formal classroom, focus groups, role-based training, and on-the job training).

Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.

Describe the awareness program for the application / system.

4 Technical Controls

4.1 Identification and Authentication

Describe the application / system's user authentication control mechanisms (password, token, and biometrics).

4.2 Logical Access Controls

Discuss the controls in place to authorize or restrict the activities of users and personnel within the application / system. Describe hardware or software features that are designed to permit only authorized access to or within the application/system, to restrict users to authorized transactions and functions, and / or to detect unauthorized activities (i.e., access control lists [ACLs]).

4.3 Public Access Controls

If the public accesses the application / system, discuss the additional security controls used to protect the application / system's integrity. What additional controls are used to protect the confidence of the public in the application/system? Such controls include segregating information made directly accessible to the public from official agency records. Others may include:

Table 4 Public Access Control Considerations

Public Access Control Considerations
Some form of identification and authentication
Access controls to limit what the user can read, write, modify, or delete
Controls to prevent public users from modifying information in the application / system Digital signatures
Copies of information for public access available on a separate application / system
Controls to prohibit the public from accessing live databases
Verification that programs and information distributed to the public are virus-free
Audit trails and user confidentiality
Application / system and data availability
Legal considerations