[System Name (SYSTEM ACRONYM)]
Interconnection Security Agreement (ISA)

Version [#]
[Month DD, YYYY]

Prepared for:
[Insert Agency Name]
[Insert Contract Number]

INTERCONNECTION SECURITY AGREEMENT

BETWEEN [ORGANIZATION A NAME]

AND

[ORGANIZATION B NAME]

[DATE OF AGREEMENT]

[Provide Organization A Name and Address]

[Provide Organization B Name and Address]

Record of Changes/Version History

ISA Template Version 1
December 1, 2014

Change/Version Number	Date of Change	Sections Changed	Description	Person Entering Change

1 INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between [Organization A Name] and [Organization B Name] are for the express purpose of exchanging data between [System Name (System Acronym)], owned by [Organization A Name], and [System Name (System Acronym)], owned by [Organization B Name]. [Organization B Name] requires the use of [Organization A Name's] [Component Name] and [Organization A Name] requires the use of [Organization B Name's] [Component Name], as approved and directed by the Director of [Department or Agency Name].

2 SYSTEM SECURITY CONSIDERATIONS

The interconnection between [System Name], owned by [Organization A Name] and [System Name], owned by [Organization B Name], is a (one-way) (two-way) communication path. The purpose of the interconnection is to deliver the [Component Name] to [Organization B Name's] [Internal Office Name] and to deliver the [Component Name] to [Organization A Name's] [Internal Office Name].

2.1 System Description

[Describe the function and data flow between the interconnected systems and the information processes for each system.]

Each Information Technology (IT) System involved in this connection is described below:

[System A Name]

[Organization Name]
[Address Location]

[System B]

[Organization Name]
[Address Location]

Note: If additional systems are used as part of the interconnection they should also be referenced in this section.

2.2 Data and Security Controls

[Provide a descriptive overview of the security controls in place to protect the exchange of data in accordance with South Carolina Information Security policies, and agency specific guidance.]

2.3 Services Offered

[Identify the specific services (e.g., electronic mail, file transfer protocol, database query, etc) that are offered as a result of this interconnection and/or state that the "Connection only exchanges data between the two interconnected systems."]

2.4 Data Sensitivity

[Provide a description of the data exchanged between (Organization A Name) and (Organization B Name). Include the sensitivity level of the data that is being exchanged.]

2.5 User Community

[Identify the users who will access the data. State the background investigations that are required to access the data. For example, "All (Organization A Name) users with access to data received from (Organization B Name) are United States citizens with a valid and

current (Organization A Name) background investigation. All (Organization B Name) users with access to data received from (Organization A Name) are U.S. citizens with a valid and current (Organization B Name) background investigation."]

2.6 Information Exchange Security

[Describe how the exchange of information is secured between systems including access control and physical security.]

2.7 Trusted Behavior Expectations / Rules of Behavior

[(Organization A Name's) (System Name) and users are expected to protect (Organization B Name's) data, and (Organization B Name's (System Name) and users are expected to protect (Organization A Name's) data, in accordance with the policies and standards of the State of South Carolina. A "Rules of Behavior" or similar document must be submitted and signed by application users for both organizations.]

2.8 Incident Reporting

[Provide a detailed process for reporting incidents by both organizations. Example verbiage to be included **with modification** as part of the Division of Information Security incident response process.

2.9 Security Parameters

[Provide an objective overview of the technical security controls; and hardware, software, firmware in place to maintain the confidentiality, integrity, and availability of the information processed between the interconnected systems.]

2.9.1 Hardware Requirements

[Identify hardware that will be needed to support the interconnection. Include communication lines, routers, firewalls, hubs, switches, servers, and workstations. Determine whether existing hardware is sufficient, or whether equipment upgrades are required to support a more secure data communication between the two organizations.]

2.9.2 Software Requirements

[Identify software that will be needed to support the interconnection. Include software for routers, firewalls, servers, and workstations. Determine whether existing software is sufficient, or whether additional software or Operating System (OS) upgrades are required.]

2.10 Operational Security Mode

[Provide a review of the operational security controls in place to secure the information processed between the interconnected systems.]

2.11 Audit Trails Responsibilities

[An example of the verbiage that could be used here is as follows: "Both organizations are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a period of [#] years or months as per organization system policies and procedures."]

2.12 Training and Awareness

[Define the specific training and awareness requirements for all authorized personnel who will be involved in managing, using, or operating the interconnection, in accordance with both organizations' policies and procedures.]

2.13 Specific Equipment Restrictions

[Identify specific organization policies and procedures that must be followed as part of the interconnected system configuration.]

2.14 Remote Connectivity

[Define the current organization policies and procedures applicable to remote connectivity as it affects the interconnected systems.]

2.15 Security Documentation

[Identify all relevant security documentation pertaining to procedures and requirements for data transmitted under this ISA.]

2.16 Escalation Procedure

[Describe the escalation process for both organizations in the event that interconnected operability and security is compromised. Describe how each organization will notify each other; the extent to which the organizations will assist each other, if at all; and the terms under which such assistance will be provided. Identify emergency points of contact.]

3 TOPOLOGICAL DRAWING

[Provide a detailed drawing that illustrates all communication paths, circuits, security components, and other components used for the interconnection.]

4 [ORGANIZATION A NAME] AND [ORGANIZATION B NAME] CONTACT LIST

The [Organization A Name] and [Organization B Name] ISA requires that an active content list be established and maintained for the categories listed in the ISA. For this purpose, the contact list has been established for each of the sections listed under the Communications section of the ISA. This contact list does not require Authorizing Official (AO) or Designated Approving Authority (DAA) signatures and updates.

[Organization A Name] contacts for disasters and other contingencies, material changes to the system configurations, new interconnections, personnel changes, and document management are as follows:

Title
Name
Organization Division
Location
Telephone Number
E-mail Address

[Organization B Name] contacts for disasters and other contingencies, material changes to the system configurations, new interconnections, personnel changes, and document management are as follows:

Title

Name

Organization Division

Location

Telephone Number

E-mail Address

5 SIGNATORY AUTHORITY

This ISA is valid for [#] years after the latest date on either signature below if the technology documented herein does not change or if there are no other intervening requirements for update. The security controls for this interconnection will be reviewed at least annually, or whenever a significant change occurs. Either party may terminate this agreement within [#] days of advance notice in writing. Noncompliance on the part of [Organization B Name] or its employees or contractors with regards to security policies, standards, and procedures explained herein will result in the immediate termination of this agreement

[Organization A Name] Authorizing Official

_____

Full Name

_____

Title

_____

(Signature) (Date)

[Organization B Name] Authorizing Official

_____

Full Name

_____

Title

_____

(Signature) (Date)