MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** **Information Technology**	**Standard:** **SECU.01.150.02**
Topic Area:	**Data Classification Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose:

The purpose of this standard is to provide the Michigan Economic Development Corporation (MEDC) Infrastructure Services Team with a Data Classification Framework that assists business units in protecting the confidentiality, integrity, and availability of their information systems and information through data classification.

Data classification is a process that prioritizes which types of data receive what level of security resources. This is done by identifying and categorizing their information and information systems based on their sensitivity, criticality and risk. Without data classification, a business unit has an increased risk of their data having inadequate security controls that may lead to a security incident or data breach. Business units that experience a security incident or data breach can suffer reputational damage, loss of customer or public confidence, and have direct costs associated with managing the incident and notifying the affected parties.

Contact/Owner:

Michigan Economic Development Corporation
Information Technology

Scope:

This policy applies to all MEDC business units that collect, process, store and/or transmit data that is under the authoritative control of the MEDC. For purposes of this document there is no distinction between information and data and while this Framework focuses primarily on the Data Classification of information systems and its data, business units can apply it to data that exists in any format (i.e., paper, e-mail, voice, video, media devices, electronic, etc.).

Standard:

This standard meets the requirements defined in the MEDC IT policy *SECU.01: Information Technology Information Security* which requires business units to identify and classify their information assets based on sensitivity, criticality, and risk. In order for business units to be in compliance with MEDC Policy SECU.01, they must implement this framework and classify their data.

This standard also complies with Control Objectives for Information and Related Technology (CoBIT) and adopts and applies data classification standards and guidelines from the following:

- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

- Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements.
- National Institute for Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- Federal Information and Information System and the Federal Information System Management Act of 2002 (FISMA).

Benefits Of Data Classification

Data classification provides many benefits to the MEDC and its business units. It helps to establish information ownership and provides a central point of control for security and access to the information. Data classification also increases the confidentiality, integrity, and availability of the data by increasing the likelihood that the data will be used in the proper context. The following are some benefits of data classification:

- Demonstrates business unit's commitment to protecting valuable information assets.
- Ensures confidentiality by restricting who has access to the data.
- Increases accuracy and integrity of information by controlling who is authorized to modify or delete the data.
- Documents location of sensitive data and protection required.
- Provides awareness of security within the business unit.
- Provides direction on the handling of sensitive data.
- Provides operational benefit by identifying critical information assets.
- Reduces security control costs by not overprotecting non-sensitive data.
- Increases security of sensitive data by ensuring that adequate security controls are identified.
- Compliance with state and federal laws, regulations, and policies.

The benefits of the framework can be summarized into the acronym ***Classify***.

- ***Compliance*** with data related business policies and procedures, legislation and audit requirements.
- ***Leaves*** MEDC Infrastructure Services Team with a uniform approach for knowing what data needs to be protected and serves as the starting point toward implementing security controls commensurate with the sensitivity and criticality of the data classified.
- ***Aligns*** business unit's missions, data, and information systems that leads to more effective and most likely, less expensive security over the most expensive data. In turn, this mitigates misuse and theft of business

units' most sensitive data which naturally reduces breach notification costs and other such costs.

- ***Shows*** that business units know what data they possess and where that data resides. The "what" and "where" of data are prerequisites to determining "how" to protect that data.
- ***Satisfies*** a preeminent goal of the MEDC for its information technology (IT) environment and information systems to be more agile in the sharing of information between business units, internal and external partners, and other entities.
- ***Integrates*** classified information/data into application and business processes more seamlessly.
- ***Fosters*** more effective compliance efforts with federal and state laws, regulatory compliance and MEDC policies.
- ***Yields*** a more reliable and consistent classification of data.

Data Classification Framework

The Data Classification Framework defined in this standard consists of eight (8) steps that provide a scalable approach for business units to classify their data:

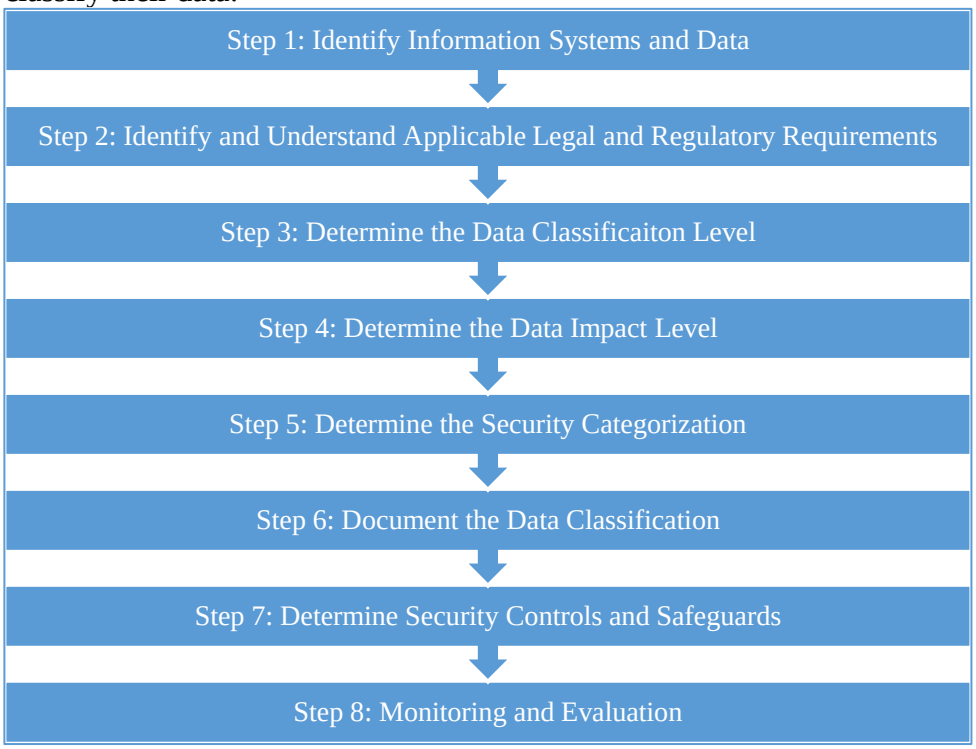

Figure 1.0: 8 Step Classification Framework

Step 1: Identify Information Systems Data

The first step in the data classification framework is for the business unit to identify their data that is collected, processed, stored and/or

transmitted. In some situations, a business unit's data may be hosted outside the MEDC network by a third party service provider. In this case, the Data Center Team is still required to classify their data and ensure that the service provider has applied the same classification level and required security controls to protect the information.

Step 2: Identify And Understand Applicable Legal And Regulatory Requirements

Each business unit may be subject to different combinations of state and federal laws, regulations or policies requiring them to protect their information. In this step of the framework, the business unit needs to identify and understand any applicable state and federal laws and regulations, policies, procedures, standards and privacy compliance requirements that require them to protect the information system and its data from unauthorized disclosure, modification, destruction, access, use or dissemination. Additional security requirements may also be found in external contractual agreements that require special handling or protection of the data.

Step 3: Determine The Data Classification Level

One of the primary objectives of data classification is to determine the proper security levels of protection. Since not all information systems or data require the same level of security controls or pose the same risk to a business unit, data classification levels are used to identify the levels of sensitivity and criticality of the information. In this step, the Data Center Team determines the Data Classification Level of the information being classified. This framework has defined four (4) data classification levels to be used by the MEDC: public, internal, confidential and restricted. Table 1.0 (shown below) provides a brief description of each data classification level:

DATA CLASSIFICATION LEVEL	DESCRIPTION	EXAMPLES
Public	Public data is information that has been explicitly approved for distribution to the public and can be disclosed to anyone without violating an individuals' right to privacy or causing any potential harm. Public data is not sensitive in context or content, and does not require special protection. If disclosed or compromised, it will not expose the MEDC to financial loss or embarrassment, compromise a competitive advantage, or jeopardize the security information.	▪ Publicly Available Financial Reports ▪ Executive Budgets ▪ Non-Exempt FOIA Documents
Internal	Internal data is information that is not sensitive to disclosure within the business unit. By default, data created, updated or stored by the business unit is considered to be Internal information intended for use by MEDC employees	▪ MEDC Policies and Procedures ▪ Customer Information ▪ Internal Announcements

	and authorized non-MEDC employees, although it may be accessed by trusted partners covered by a non-disclosure agreement. This information shall be shared internally to further internal operations, lower costs, prevent duplication, and otherwise enhance the condition or operation of MEDC systems.	and Communications ▪ Internal Phone Directories and Organizational Charts
Confidential	Confidential data is sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an MEDC. Confidential data may include personal identifying information (PII) or confidential non-public information that relates to MEDC business. Confidential data should only be made available to authorized personnel on a need-to-know basis and should require a signed non-disclosure agreement.	▪ Social Security Numbers ▪ Credit Card Numbers ▪ Civil Investigative Data ▪ Criminal History Data ▪ Confidential Business Information ▪ Financial Statements ▪ Health and Medical Records
Restricted	Restricted data is information that is extremely sensitive and any disclosure or corruption could be hazardous to life or health, cause extreme damage to integrity or image, and/or impair the effective delivery of services. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship and major economic impact. Restricted data can be made available to named individuals or specific positions on a need-to-know basis.	▪ Sensitive Law Enforcement Data ▪ Investigative Records and Communications Systems ▪ Disaster Recovery and Business Continuity Plans ▪ Protected Critical Infrastructure Information

Table 1.0: Data Classification Level

Step 4: Determine The Data Impact Level

In this step, the ***Data Impact Level*** is determined by assigning a potential impact level of High, Moderate or Low to each security objective for each data type or information system being classified. The security objectives used in this framework are confidentiality, integrity and availability and are defined below in FIPS 199 Potential Impact Definitions for Security Objectives.

The potential impact is the outcome if the data and/or information system were subject to a security incident. A security incident may include events that do not constitute a breach or actual compromise, but pose a security risk to MEDC or is a violation of an explicit or implicit law, regulation or policy which may increase the risk of a security breach. The following are

several ways in which a security incident could lead to a data security breach:

1. Lost or stolen laptops, iPads, Smartphones or other types of electronic devices.
2. Unauthorized access to information data or information systems.
3. Unauthorized sharing of data.
4. Unauthorized access to user accounts or password sharing.
5. Noncompliance with state and federal laws and regulations, policies, procedures and standards.
6. Noncompliance with contractual obligations regarding the security of the data and/or information system.

Table 2.0 is an excerpt from **Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems** and summarizes the potential impact definitions for each security objective (confidentiality, integrity and availability). This table is used when determining the data impact level for each data type or information system.

POTENTIAL IMPACT			
SECURITY OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542][1]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

[1] United States Government Publishing Office, Title 44, Section 3542, January 15, 2015. https://www.gpo.gov/fdsys/pkg/USCODE-2012-title44/pdf/USCODE-2012-title44-chap35-subchapIII-sec3542.pdf (accessed 09/21/16).

Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 2.0: Potential Impact Definitions For Security Objectives

Step 5: Determine The Security Categorization

The security category of an information type can be associated with both user information and system information[2] and can be applicable to information in either electronic or non-electronic form. The purpose of this step is to establish the security categorization of the data being classified. Security categorization is the basis for the proper security control selection to protect the information and is determined at the data type and information system level. Once the data impact levels have been selected for each security objective, the security categorization is assigned to each information system or data type as defined in Table 3.0 below.

SECURITY CATEGORIZATION	IMPACT DESIGNATION
LOW	An information system and/or data type in which all ***three*** security objectives, confidentiality, integrity and availability, are assigned a FIPS 199 potential impact value of ***low***.
MODERATE	An information system and/or data type in which ***at least one*** security objective, confidentiality, integrity and availability, are assigned a FIPS 199 potential impact value of ***moderate***, and ***no security objective is assigned a FIPS 199 potential impact of high.***
HIGH	An information system and/or data type in which ***at least one*** security objective, confidentiality, integrity and availability, are assigned a FIPS 199 ***potential impact value of high***.

Table 3.0: Security Categorizations

Security Categorization Of An Information Data Type

Establishing the appropriate security categorization for a data type merely requires determining the potential impact for each security objective associated with the specific data type and using the highest values from the impact designations (see Table 3.0: Security Categorizations).

Example 1 (Figure 2.0): A law enforcement agency is managing extremely sensitive investigative information. The data owner determines that the potential impact from the loss of confidentiality is High, the potential impact from the loss of integrity is Moderate and the potential impact from a loss of availability is Moderate. The resulting categorization for this data is defined as:

[2] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February, 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (accessed 09/21/16).

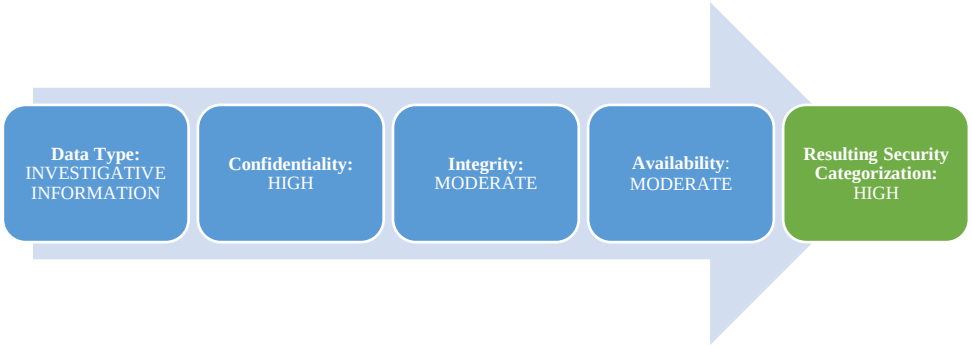

Figure 2.0

- Based on the security objectives and the overall data impact level, the Security Categorization for this data type would be ”High.”

SECURITY CATEGORIZATION APPLIED TO AN INFORMATION SYSTEM

Determining the security category of an information system requires analysis of all the security categories of all data types resident on the information system. For an information system, the potential impact values assigned to the security objectives, confidentiality, integrity, and availability, shall be the highest values from among those security categories that have been determined for each type of resident data on the information system (see Table 3.0: Security Categorizations).

Example 2 (Figure 3.0): An information system used by multiple departments for large contracts contains both sensitive contract information and non-sensitive administrative information.

The data owners of this system have determined that for the contract information, the potential impact from a loss of confidentiality is Moderate, the potential impact from a loss of integrity is Moderate, and the potential impact from a loss of availability is Low. For the Administrative Information, the potential impact from a loss of confidentiality is Low, the potential impact from a loss of integrity is Low, and the potential impact from a loss of availability is Low. The overall security categorization of this information system would be as follows:

DATA TYPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Contract Information	Moderate	Moderate	Low
Administrative Information	Low	Low	Low

Figure 3.0

- Categorization for this information system would be “Moderate.”

STEP 6: DOCUMENT THE DATA CLASSIFICATION

In this step the MEDC Data Center Team documents the outcome of the data classification process. The documentation would include the information or information system being classified, data classification

level, data impact level, security categorization, approvals, and supporting rationale for the classification. Documentation by the MEDC Data Center Team should be used by or made available to the appropriate personnel who support the business unit and their information systems, such as the Infrastructure Services, Director, Chief Information Officer, and auditors. This information is used to support the following activities: audits, business impact analysis, enterprise architecture solution assessments, system designs, security plans, risk assessments, business continuity, disaster recovery planning, and system interconnections agreements.

STEP 7: DETERMINE SECURITY CONTROLS AND SAFEGUARDS

The purpose of this step is to determine the security controls and safeguards required to protect the data. The minimum baseline security controls are the starting point for the security control selection process, and are the basis from which controls and control security protection required for the information system. Additional security controls that are not addressed in the NIST 800-53 Security Controls may be required based on regulatory compliance.

STEP 8: MONITORING AND EVALUATION

Data classification is not a project but a program that will change the way business units manage their data. Business units are required to continually monitor their data classification program by periodically evaluating and reevaluating the classification of their data to ensure that new unclassified data has not surfaced, or that the classification of assigned data is still appropriate based on legal and contractual obligations, as well as its value and use to MEDC.

In some situations, a business unit may de-classify the data by removing data elements such that the remaining data does not meet the current classification. For example, a business unit may have a data type with name, address, and social security number. By removing the social security number, the data type is no longer sensitive and therefore does not require a higher level of security protection.

If the data classification of any information system and/or its data has changed, an analysis of security controls should be performed to determine whether existing controls meet the legal and contractual obligations. If gaps are found in existing security controls, they should be corrected in a timely manner.

ROLES AND RESPONSIBILITIES

DATA CENTER TEAM

- Update the Data Classification Framework, keeping it current with industry standards and guidelines.
- Guide the framework standard through the MEDC policy process.

- Provide guidance to business units, MEDC Infrastructure Services Team, and the Chief Information Officer on the implementation and use of the framework.
- Ensure that the data classification is built into the MEDC security plan.
- Understand the business unit's information and information systems and network, data that is collected, processed, stored, and transmitted.
- Promote a culture of data classification and protection within their business unit.
- Ensure that a data classification policy and procedure is implemented within the business unit.
- Ensure employees are aware of the MEDC Data Classification Framework and business unit policies, standards, and procedures classifying and protecting sensitive data.
- Understand regulatory compliancy requirements regarding use and dissemination of sensitive data.

INFRASTRUCTURE SERVICES, DIRECTOR

- Understand the business unit's information, information systems and network, data that is collected, processed, stored, and transmitted.
- Collaborate with the Data Center Team to define, implement, and review appropriate security controls with data classification to ensure that information systems and data are properly protected from unauthorized access, modification, disclosure, and destruction.
- Develop access control procedures for approving, managing, and revoking rights to the information.
- Periodically review access rights to ensure they are still appropriate with system end users' job requirements.
- Assign proper classification level to their information and information systems using the Data Classification Framework.
- Monitor and reevaluate data classification on a periodic basis to ensure data is still classified properly.
- Manage and maintain the data classification documentation in a manner that is easily identifiable, accessible and secure for business units requiring access to it.
- Educate business units on the proper handling and protection for the different types of data classifications levels.
- Ensure that any data and/or information systems that are hosted by a third party service provider have the classification level applied and that the proper security controls to protect the information have been implemented.
- Communicate data classification and security control requirements to the Chief Information Officer and system end users.

CHIEF INFORMATION OFFICER

- Ensure that data classification is taken into account when defining security requirements for infrastructure and information systems.
- Work with the Infrastructure Services, Director to understand their legal, regulatory or business requirements and how their data has been classified.
- Understand required security protection for collection, processing, storing and transmission of the information systems and/or data they support.
- Inform the Data Center Team and Infrastructure Services, Director as to the best operational and technical controls necessary to protect their data in accordance with its data classification level, security objectives, and security categorization.
- Implement and monitor approved security controls in accordance with its data classification level, security objectives, and security categorization.
- Ensure hosting access control procedures are implemented for approving, managing and revoking rights to the information.
- Utilize the recommended security controls from the National Institute for Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems, and other safeguards and countermeasures to mitigate the risk to the business unit's information systems and data.

TERMS AND DEFINITIONS:

Availability

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to, or use of information or an information system.

Business Unit

A unit of organization within the MEDC.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Data

For the purpose of this standard, data and information are used interchangeably. Data is the collection of all MEDC and/or Business Unit information.

Data Owner

Official person, usually a member of senior management, with statutory, management or operational authority for the information, and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the Data Owner is responsible for establishing the rules for appropriate use and protection of the information.

Data Type

Data type, also referred to as information type, is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), as defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Framework

A framework is a layered structure intended to serve as support or guidance for the building of programs, standardization of organizational activities, and the communication of how they are interrelated to produce the program objectives for the organization.

Information Security

For the purpose of this standard, information is not limited to data contained in computer systems, but is inclusive regardless of where it resides within the business unit, what form it takes (i.e., electronic, printed, etc.), what technology was used to handle it, or what purpose it serves.

Information Type

Information type, also referred to as data type, is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), as defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Information Technology Resources

Computers, storage peripherals, network equipment and wiring, network-attached printers, and fax machines.

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Risk Assessment

Risk assessment is a process which determines what information resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Security Category

The categorization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Categorization

The process of determining the security category for information or an information system.

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Objective

Confidentiality, integrity or availability.

Security Plan

Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

MEDC Network and Information Technology Customers

Same as Data Custodian.

Exceptions:

All exceptions for this standard shall be in compliance with the Administrative Guide Policy *AUTH.01: Enterprise Information Technology*.

Approving Authority:

- Executive Order No. 1999-1, formation of the MEDC.
- Executive Order No. 1999-1 and assigning IT staff to the MEDC for the purpose of the administration of MEDC technology usage.
- The *AUTH.01: MEDC Information Technology* policy is the mechanism for establishing an enterprise approach to IT management and serves as the overarching umbrella policy for MEDC information and assets

Authoritative Policies:	SECU.01
Associated Procedures:	Not Applicable

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer	November 17, 2016

Author:	Approver:	Approval Date:	Description of Change(s):
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy approval.