THE DATA CENTER

STATEMENT PRINTING • DIRECT MAIL • DATA SERVICES

The Data Center
Computer Information Systems
Security Policies and Procedures Framework
(TDC CIS SPPF)

Prepared by: Dan Hansen

Revision: 05/24/2013

Version: 4.5

Approved by: TDC CIS SPPF Review And Adoption Team

TABLE OF CONTENTS

1. Purpose Statement: Security Policy and Procedure Framework

This document defines the security policies and procedures that serve to; (i) expand upon the current company-wide security policies and procedures (Appendix A); providing a framework for authorized CIS Systems staff to achieve a comprehensive approach for the development, implementation, monitoring, and control of all organization computer information systems (CIS Systems) directly impacted by, and associated with, receiving, transferring, handling, processing, and storing customer data; (ii) establish a security strategy tool for meeting The Data Center's (TDCs) compliance obligations and security standards with regard to CIS Systems; (iii) document and provide a detailed understanding of responsibilities with regard to TDCs CIS Systems compliance obligations and security standards and associated risks; (iv) serve as a reference point to ensure the establishment, implementation, and enforcement of the security policies and procedures set forth within this framework.

The development of this framework, referred to as The Data Center Computer Information Systems Security Policies and Procedures Framework (TDC CIS SPPF), is informed by seventeen security-related areas defined by the National Institute of standards and Technology (NIST), found in the Federal Information Processing Standards Publication (FIPS) Publication 200, with regard to protecting the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by all TDC CIS Systems directly impacted by, and associated with, receiving, transferring, handling, processing, and storing said data. The seventeen security-related areas are as follows: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity.

TDC CIS SPPF, serves to guide the application and implementation of our security policies and procedures to TDC CIS Systems, how users interact with TDC CIS systems, and accounts for every aspect of all data, applications, operating systems, hardware, security mechanisms, and security devices associated with TDC CIS Systems; forming an end-to-end Security Infrastructure and Architecture (SIA) platform-solution for TDC and its customers.

2. TDC CIS SPPF: Roles and Responsibilities

ROLES	RESPONSIBILITIES
TDC CIS SPPF Review And Adoption Team: -Kim Kendall; President/ Owner -Derek Toronto; Programmer/ Manager -Dan Hansen; CIS Infrastructure/ Network Admin	Responsible for review and approval of CIS SPPF policies and documentation: Including but not limited to, revisions, updates, inclusions, exclusions, replacement and new CIS SPPF documentation. Ensuring company-wide adoption and compliance with security policies and procedures set forth herein.
President/ Owner: -Kim Kendall	Approval of TDC CIS SPPF documentation. Compliance assurance and enforcement of TDC CIS SPPF.
IT Personnel and Management, Data Programming, and Print Production Manager: -Derek Toronto	Responsible for source, and live data handling and programming, variable print-data; data residing on the inside boundary of the internal company-facing TDC SIA component. Custom programming and associated programming and data integrity. Accuracy of data and final print. Scheduling of print equipment time and print production operators. Building of internal company-facing hand-off and production CIS Systems. Approval of TDC CIS SPPF documentation. Compliance assurance and enforcement of TDC CIS SPPF of production facilities.
IT Personnel and Management, CIS Infrastructure and Network Admin: -Dan Hansen	Responsible for building, maintaining, and managing the security infrastructure and architecture (SIA) backbone, external, customer-facing infrastructure, and internal, company-facing custom hand-off processes components pursuant to production systems. Data handling and programming of data on external, customer-facing of the TDC SIA component. Ensuring security mechanisms are in place and in compliance pursuant to TDC CIS SPPF approved documentation. Drafting, updating, and approval of TDC CIS SPPF documentation. Compliance assurance and enforcement of TDC CIS SPPF of overall TDC SIA.

3. TDC CIS SPPF: Review and Update

TDC CIS Systems SPPF will be reviewed at least bi-annually by TDC CIS SPPF Review and Adoption Team with intent to achieve the following objectives:

1. TDC meets compliance obligations with regard to CIS Systems security standards.
2. TDC CIS Systems framework maintains its relevance to established standards.
3. TDC continues to meet its CIS Systems security obligations and responsibilities.

4. Scope: TDC Security Infrastructure and Architecture (TDC SIA)

The policies and procedures set forth within TDC CIS SPPF, when applied to TDC CIS Systems, serve to inform and guide the development, interaction, and function of TDC CIS Systems; thereby forming TDC Security Infrastructure and Architecture (TDC SIA). It is within the scope of TDC SIA that TDC CIS SPPF will be applied.

4.1 TDC SIA: Overview

The Data Center invests significant time and resources ensuring the security and protection of customer data with regard to confidentiality, integrity, authenticity, and availability of information processed, stored, and transmitted by our CIS Systems. This investment has culminated in the establishment of an end-to-end SIA platform-solution for TDC and its customers.

4.2 TDC SIA: Model

TDC SIA is comprised of the internal company-facing component, and the external customer-facing component. Together both components form an end-to-end solution facilitating the means to achieve confidentiality, integrity, authenticity, and availability of information processed, stored, and transmitted to and from TDC CIS Systems.

4.3 TDC SIA: Internal company-facing component

TDC SIA internal company-facing component is comprised of a server farm, functioning as the data hub and primary intermediary between TDC and its customers. And the internal hand-off infrastructure which acts as an extension of the internal data hub mechanisms and component and associated production-facility CIS Systems and production staff.

4.4 TDC SIA: External Customer-Facing Component

TDC SIA external customer-facing component is comprised of the overlapping company-facing and customer-facing mechanisms of the internal server farm component, functioning as the data hub and primary intermediary between TDC and its customers. Unless an alternate and secure data transfer method is requested, arranged, and furnished by the customer, TDC , or third-party vendor, all customer's requiring a secure method for data transfer will be accommodated and provided the necessary information to establish a secure (permanent or ad-hock SIA) connection with TDC SIA. Customer-established connection to TDC SIA will be via customer initiated upload/download to TDCs sFTP, or FTPS servers, which function as TDCs SIA customer-facing component and primary data hub and intermediary for transferring and receiving all customer-sensitive data. TDC SIA customer-facing component functions as the security intermediary providing the primary mechanism by which customer data will be transferred either (a) from the customer, to TDC SIA customer-facing component, via customer-initiated upload or (b) from the customer, from TDC SIA customer-facing component, via customer-initiated download. In either instance, any and all data transfer activity, either to or from TDC SIA, will be initiated by the customer.

4.5 TDC SIA: End-To-End Solution

TDC SIA internal company-facing component and external customer-facing component form an end-to-end solution facilitating the means to achieve confidentiality, integrity, authenticity, and availability of information processed, stored, and transmitted to, or transmitted from, TDC CIS Systems.

4.5.1 External Customer-facing

The customer-facing component provides the platform for customers to interface with TDC SIA where only secure data traversal will occur. The customer-facing component is comprised of TDC virtual server farm, housed behind a multi-layer security architecture: (i) Layer 1 is comprised of programmed cisco gateway devices providing; (a) PAT translation, and; (b) firewall security; allowing for known protocols pointed to specified internal services. (ii) Layer 2 is comprised of programmed cisco security appliances, only allowing known customer hosts and protocols to reach the server farm and associated internal services; specified at the first security layer. (iii) Layer 3 is comprised of the specified server platform internal firewall, allowing for only specific protocol traffic and services. (iv) Layer 4 is the authentication mechanism of a unique user name and password combination assigned to each individual user account granting access to either a sFTP, or FTPS server session. (v) Layer 5 implements either an ssl/tls encryption-authentication mechanism or an ssh public/ private key encryption-authentication mechanism; determined by the customer's chosen access method and server session.

4.5.2 Internal Company-facing

The company-facing component provides the internal mechanisms facilitating hand-off from the customer-facing component, allowing for the secure receipt, programming, processing, printing, and storage of customer data. From the point a customer-initiates and uploads data to the customer-facing component, said data will temporarily exist within a secure and isolated user account directory within the server farm where it will be removed via custom logic processes and handed-off to internal operations. The hand-off is achieved via isolated data streams from the server farm to a secure queuing platform. Internal staff do not directly access temporarily stored server farm data.

From the hand-off point customer data is sent directly to a Network Allocation Storage (NAS) queue where access is only achievable to authorized, internal personnel, possessing exclusive access rights to queuing system. From this point, the data will be removed and placed on the programmers secure system, for appropriate programming and processing. Only the programmer will see the raw source data. From this point, the programmer will follow the print data to completion or hand off print duties to authorized print operators. Once the print order is completed, the original source data will be encrypted and either; (a) get pushed into the backup queue to be securely stored and archived, or; (b) removed from all systems and permanently destroyed ; as per customer request.

5. TDC CIS SPPF Applied

TDC receives, handles, processes, and stores customer-sensitive data. As such a security framework for developing, implementing, monitoring, and controlling, the security of associated data and systems is established throughout this document to ensure the integrity, confidentiality, availability, and safe storage of customer-sensitive data and systems.

TDC company-wide security policies and procedures, found in Appendix A of this document, provide the general security statements that guide TDC CIS security policy. The security areas, found in the next section, provide the necessary detail toward implementing and applying these company-wide policies to the CIS Systems infrastructure; achieving an end-to-end SIA. TDC SPPF Security Areas, as informed by FIPS Publication 200, cover a wide scope of management, operational, and technical areas and as such function to foster company-wide awareness, adoption, participation, implementation, and compliance.

6. TDC CIS SPPF Requirements

FIPS Publication 200 Security Areas	TDC CIS SPPF Requirement
Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise (NIST, 2006, p.2).	TDC SIA Access Control will be achieved via multi-layer security architecture. All systems within the scope of TDC SIA: (1) Production facility and TDC CIS Systems; Reside within the production facility. The production facility encompasses the production floor, production offices, and server room. The customer-facing external component (ie. server farm) resides within a locked cabinet housing, which in turn is behind electronically locked doors; behind an electronically locked production facility. The entire floor-space is contained within a secured building implementing multi-layered physical security architecture (Refer to: Physical and Environmental Protection). (2) Accessibility of production facility and TDC CIS Systems; Critical systems within the scope of TDC SIA will be accessible only to lead programmer and systems admin. Production facility systems will be accessible only to select and authorized production staff, lead programmer and systems admin. (3) Networking infrastructure and TDC CIS Systems; (i) Layer 1 will be comprised of Cisco gateway appliance providing a) PAT translation, and b) firewall security; allowing for known protocols

	pointed to specified internal services. (ii) Layer 2 will be comprised of cisco security appliances, allowing, only, known customer hosts and protocols to reach the server farm and associated internal services; specified at the first security layer. (iii) Layer 3 will be comprised of the specified server platform internal firewall, allowing for only specific protocol traffic and services. (iv) Layer 4 will constitute the authentication mechanism of a unique user name and password combination assigned to each individual user account granting access to either an sftp or ftps server session. (v) Layer 5 will implements either an ssl/tls encryption-authentication mechanism or an ssh public/ private key encryption-authentication mechanism; determined by the customer's chosen access method and server session (4) Data handling, data access, system access, and TDC CIS Systems; Data files and systems can only be accessed by our programmers and select, and authorized production staff. Unless special production arrangements are made, sensitive customer data in raw form (ie. source data from the customer) will be handled by our lead programmer, only. This provides access control where sensitive data has been removed from further access, manipulation, or network traversal where; (a) source data is pulled either; (i) directly from the customer to the programmer's system, via an agreed upon, secure method, or; (ii) source data will be pulled from, and removed from, the internal NAS queue, by the programmer, to the programmer's system. After the initial data programming and processing has occurred data in the form of a document print file will be moved, from the programmer's system, by the programmer, and placed directly to the production printing queue. From this point, the original source data will be encrypted and either; (a) backed-up to physical media and stored within TDC secured media storage apparatus, or;(b) destroyed via special system erasure utility and permanently removed from the programmer's system.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities (NIST, 2006, p.2).	Company wide security policies and procedures, found in Appendix A, will function to promote company-wide awareness to all TDC staff. This document, or TDC CIS SPPF, will function as a primary vehicle to promote awareness, and provide a framework for authorized CIS Systems staff to achieve a comprehensive approach for the development, implementation, monitoring, and control of all TDC CIS Systems directly impacted by, and associated with, receiving, transferring, handling, processing, and storing customer data. Establish a security strategy tool for meeting TDC compliance obligations and security standards with regard to CIS Systems. Document and provide a detailed understanding of responsibilities with regard to TDCs CIS Systems compliance obligations and security standards and associated risks. Serve as a reference point to ensure the establishment, implementation, and enforcement of the security policies and procedures set forth within this framework. Additionally, annual, and as necessary, meetings with all necessary staff is conducted to ensure each staff member is aware of individual responsibilities with regard to TDCs CIS Systems compliance obligations and security standards and associated risks.
Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions (NIST, 2006, p.2).	Refer to Appendix A; Systems Auditing: Monitoring and Auditing of CIS Systems Infrastructure.
Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in	Refer to Appendix A; Systems Auditing: Monitoring and Auditing of CIS Systems Infrastructure.

organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls (NIST, 2006, p.2).	
Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems (NIST, 2006, p.3).	1) TDC CIS Systems' configurations are managed, backed, stored, and maintained by IT management only. The configurations and respective device details are stored in a local database management system which is username and password protected and accessible by IT management only. Additionally, for TDC CIS Systems detail, policy, and procedure refer to: 2) APPENDIX A Company-Wide Security Policy; Security Strategy: TDC CIS Systems high-level overview security strategy TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal Systems Auditing: Monitoring and auditing of CIS Systems infrastructure and backup schedule Backup Schedule Auditing: Monitoring and auditing of automated backup routines Electronic Media Protection: TDC CIS Systems electronic media use and storage policy. 3) APPENDIX B TDC CIS Systems: Maintenance Lifecycle and Purchasing Strategy.
Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations (NIST, 2006, p.3).	Refer to APPENDIX C TDC Disaster Recovery and Business Continuity.
Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems (NIST, 2006, p.3).	All users of TDC CIS Systems will be *identified* via unique username; associated with one specific user and user account; known only to that one specific, and individual user. All users of TDC CIS Systems will be *authenticated* via specific and unique password; associated with one specific user and user account; known only to that one specific, and individual user. All TDC CIS Systems within the scope of TDC SIA

	reside within a windows environment. Access is contingent upon username and password authentication via either; (1) domain-level limited user account credentials, or; (2) local-level limited user-account credentials; allowing accessing to limited accounts and functionality, only. The method and model used will be contingent upon the designated production function, purpose, area, and scope of the individual accessing production machine or system. Each machine or system within TDC CIS Systems production environment will be designed and authorized for a specific production-related purpose and is configured with the least-privileged access rights. Systems will be accessed on an as-need basis to perform duty-specific functions. Each system will be built specifically to its function where purposed hardware, software, and firmware will be installed and applied by IT management only. Each system's use will be user-specific; unless special design and implementation exception is made due to production necessity, restrictions, or requirements. Administrator account access to TDC CIS Systems, for the express purpose of performing system's modifications, maintenance, and specific updates will be available and performed by IT management only.
Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities (NIST, 2006, p.3).	Refer to APPENDIX A; Incident Response: TDC CIS Systems Security Incident Procedures.
Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance (NIST, 2006, p.3).	1) Refer to APPENDIX B TDC CIS Systems: Maintenance Lifecycle and Purchasing Strategy. 2) Refer to APPENDIX A Company-Wide Security Policy; (i) Security Strategy: TDC CIS Systems high-level overview security strategy (ii)TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal

	(iii) Systems Auditing: Monitoring and auditing of CIS Systems infrastructure. (iv) Backup Schedule Auditing: Monitoring and auditing of automated backup routines (v)Electronic Media Protection: TDC CIS Systems electronic media use and storage policy.
Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. (NIST, 2006, p.3).	Refer to APPENDIX A; Electronic Media Protection: TDC CIS Systems electronic media use and storage policy.
Physical and environmental protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems (NIST, 2006, p.3).	Refer to APPENDIX C TDC Disaster Recovery and Business Continuity.
Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. (NIST, 2006, p.3).	This, TDC CIS SPPF, and APPENDIX A Company Wide Security Policy, function as living security and procedures policy documents. This document expands the security policies of Appendix A, functioning as a framework; facilitating the implementation of TDC security policies and procedures set-forth in Appendix A.
Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures (NIST, 2006, p.3).	TDC has achieved a hiring history largely comprised of word of mouth and personal reference personnel. This has been made possible by; (a) TDC has maintained and enjoyed a smaller and managed organizational scope of operations and; (b) TDC has a historically low employee turnover rate. 90% of current staff members have been with TDC since the company inception; 18 year history. However, TDC maintains a zero tolerance standing for security breach with regard to private, confidential, and financial information, and will terminate for any such reason. Additionally, TDC will conduct drug testing at random and on an as necessary basis. TDC partners with DSS

	Investigations for annual background checks on new hires, and current employees on an as necessary basis. Background checks are conducted through LexisNexis.
Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information (NIST, 2006, p.3).	Refer to APPENDIX D Risk Assessment
System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization (NIST, 2006, p.3).	1) Refer to APPENDIX A Company-Wide Security Policy; (i) Security Strategy: TDC CIS Systems high-level overview security strategy. (ii) TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal. (iii) Systems Auditing: Monitoring and auditing of CIS Systems infrastructure. (iv) Backup Schedule Auditing: Monitoring and auditing of automated backup routines. (iv) Electronic Media Protection: TDC CIS Systems electronic media use and storage policy. (v) Incident Response: TDC CIS Systems security incident procedures. 2) Refer to APPENDIX B TDC CIS Systems: Maintenance Lifecycle and Purchasing Strategy
System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems (NIST, 2006, p.4).	1) Refer to, Scope: TDC Security Infrastructure and Architecture (TDC SIA) 2) Refer to APPENDIX A Company-Wide Security Policy; (i) Security Strategy: TDC CIS Systems high-level overview security strategy. (ii) TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal. (iii) Systems Auditing: Monitoring and auditing of CIS Systems infrastructure. (iv) Backup Schedule Auditing: Monitoring and auditing of automated backup routines. (iv) Electronic Media Protection: TDC CIS Systems electronic media use and storage policy. (v) Incident Response: TDC CIS Systems security incident procedures.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response (NIST, 2006, p.4).	Refer to APPENDIX A Company-Wide Security Policy; (i) Security Strategy: TDC CIS Systems high-level overview security strategy. (ii) TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal. (iii) Systems Auditing: Monitoring and auditing of CIS Systems infrastructure. (iv) Backup Schedule Auditing: Monitoring and auditing of automated backup routines. (iv) Electronic Media Protection: TDC CIS Systems electronic media use and storage policy. (v) Incident Response: TDC CIS Systems security incident procedures.

Appendix A Company-Wide Security Policy

The following inclusion provides the current company-wide, high-level security policies and procedures detail from original document: ***The Data Center Computer Information Systems (CIS) Security Policies, Procedures, and Change Control.*** *Original circulation:* 07/06/2011.

Purpose statement: Security Policies, Procedures, and Change Control

All policies, procedures, and change control measures defined within this document apply company-wide to all TDC CIS systems infrastructure, and therefore to all persons employed by TDC utilizing any component, and or system that comprises TDC CIS systems infrastructure.

TDC CIS infrastructure encompasses all computers, computer peripherals, networking device hardware including routers, switches, wireless access points, cables, and security devices, operating systems, and associated software.

Any and all security policies will be adhered to by all persons employed by TDC.

Security Strategy: TDC CIS Systems high-level overview security strategy

This policy functions as TDC CIS Systems standard for achieving a secure infrastructure environment. Additionally, this policy serves to ensure limited and secure access to TDC operations-critical CIS Systems that may contain sensitive and confidential information. Any and all procedures indicated will be evaluated, performed, implemented, and maintained by IT management only.

1. All systems must be hardened based on the principal of least-privileged access via the following:
    a) All network infrastructure hardware including routers, switches, wireless access points, and security devices will be secured via in-band ACL restrictions, and out-of-band console password protection, disabled SSID broadcasting, and AES PKI.
    b) Passwords will be generated and controlled by IT management. Passwords will be alpha-numeric, have a minimum length of eight characters and consist of at least one number and one symbol; preferably a longer phrase-based implementation.
    c) Local administrator accounts disabled or password protected.
        i. Administrator accounts will be accessible to authorized IT management only.
        ii. Administrator accounts will be used for the purposes of new builds, modifications to existing software, major upgrades, general system maintenance, and to facilitate infrastructure changes.
    d) User or limited access accounts, only, will be implemented for all production systems and used as the primary method for interaction with any CIS System, for any and all daily operational use.
    e) All CIS System OS patches and updates maintained and applied on a weekly-basis, minimum.
    f) All CIS System OS firewalls must be operational and implementing the least-privileged/ fewest-possible exceptions for each particular system to perform its designated function.

g) All CIS System OS protected by up-to-date end-point virusware protection.

TDC CIS Systems infrastructure: Planning, building, installing, modifying, and removal

This policy serves to ensure limited and secure access to TDC operations-critical CIS Systems that may contain sensitive and confidential information. Additionally, this policy ensures uniform processes and standards will be applied to the implementation of TDC CIS Systems infrastructure. Any and all procedures indicated will be evaluated, performed, implemented, and maintained by IT management only.

TDC CIS Systems infrastructure includes, but is not limited to, all hardware and software which comprise any component(s) directly or indirectly (domain, local, or remote) connected to TDC network, or on TDC premises, and owned by TDC. The planning, building, installing, modifying, and removal of TDC CIS Systems include:

1. Any and all OS service-pack updates
2. Any and all OS modifications of servers, and workstations: including firewall, registry, user accounts, domain or local security policies.
3. Any and all domain or local user accounts and passwords.
4. Any and all standing/ installation/ joining to network of new machines (server, workstations, mobile devices, and peripherals).
5. Any and all installation, removal or modification of application software: including but not limited to email, browser add-on (if necessary), third-party software.
6. Any and all endpoint security software (virusware, malware protection).

Systems Auditing: Monitoring and auditing of CIS Systems infrastructure

This policy serves to ensure TDC CIS Systems infrastructure security and health by monitoring systems and network activity for unusual, unexpected, or unauthorized: threats or traffic patterns, and access to systems or devices. Any such activity will be evaluated and escalated to the appropriate level of mitigation. Appropriate procedures for security threats will be found in this document under section: Incident Response: TDC CIS Systems security incident procedures.

Systems auditing ensures the implementation of security mechanisms and components are functioning as expected. Any audit documentation will be retained for review and baseline comparison. Any system audit and security logs will remain intact for historical record and baseline comparison. Any and all procedures indicated will be evaluated, performed, implemented, and maintained by IT management only.

1. Audits of network traffic, traffic patterns, and packet analysis will be conducted on a regular, and as necessary, basis via gateway, router, patch panel, and switch LAN segment.
2. System services and port scans will be conducted on a regular, and as necessary, basis to document, establish, and correct, if necessary, identified system vulnerabilities.
3. An established footprint of network traffic is used as a baseline for monitoring and maintaining regular and established network usage.
4. Regular inspection of critical systems access, security, and audit logs will be conducted on a regular, and as necessary, basis.

5. Virusware detection logs will be regularly surveyed for intrusion and un-authorized activity.
6. Visual inspection of hardware and cabling will be performed each day.

Backup Schedule Auditing: Monitoring and auditing of automated backup routines

This policy functions to ensure data storage integrity and business continuity with regard to monitoring and inspecting back up logs for the successful completion of automated processes. These procedures will be evaluated, performed, implemented, and maintained by IT management only.

- Inspection of nightly backup logs and backup integrity assessment will be performed and monitored each day.

Electronic Media Protection: TDC CIS Systems electronic media use and storage policy

TDC Electronic Media Protection policy functions to ensure the secure safeguarding and protection of electronic removable storage media that maintains electronic sensitive information.

1. Any and all sensitive data, residing on fixed, removable, or mobile device media, will be encrypted using TDC approved encryption tools.
2. If sensitive data is to be retained for any given period, said data will be encrypted prior to writing or archiving to storage medium.
3. Disk drives and removable electronic media must be sanitized prior to any final disposition or reuse.
4. Sanitization method policy is that to destroy any and all data contained via third-party data erasure utility; prior to reuse or disposition.
5. Removable media or mobile devices that are considered lost due to negligence, accident or theft, containing suspected unencrypted sensitive information will be reported IT management in order to initiate mitigation, and assess scope of potential damages that could result from possible unauthorized access and disclosure.
6. Destruction of electronic removable media must be documented. The documentation must describe the destruction process used to physically damage the medium so that it is not usable by any device that could read that medium.
7. Violation of this policy may result in disciplinary action, and including possible termination of affected employees. Additionally, individuals are subject to civil and criminal prosecution or other legal action. They may also be held financially liable.

Incident Response: TDC CIS Systems security incident procedures

Any and all suspicious or unauthorized activity with regard to Information Systems security will be reported to IT management. All responsible IT staff will take immediate action to resolve, and prevent any such reoccurrence.

Any and all suspicious or unauthorized activity with regard to Information Systems security will be assessed on a case-by-case basis to determine the appropriate course of action to ensure against reoccurrence and reported to Human Resources for evaluation and immediate enforcement of corrective action, punitive measures, or termination of employment.

1. Incident: Identification of an incident.
    A. Any and all of the following policies and reporting procedures will be adhered to by all employees, guests, or users, of TDC CIS Systems. Any of the following will require immediate action:
        (i) Data theft: loss of information confidentiality
        (ii) Data damage: unauthorized modification; compromise of information integrity
        (iii) Theft of any physical IT asset including computers, storage devices, etc.
        (iv) Damage to any physical IT assets including computers, storage devices, etc.
        (v) Misuse of any physical IT asset
        (vi) Misuse of any IT services, information, or data.
        (vii) Infection of systems by unauthorized or hostile software.
        (viii) Unauthorized access or suspected attempt at unauthorized access.
        (ix) Unauthorized modification to IT assets: hardware, software, configuration.
        (x) Unusual system behavior.
        (xi) Responses to intrusion detection messages or alarms.

2. Containment: Taking action
    A. All containment and escalation procedures will be performed by IT management only.
    B. Immediate action will be taken to prevent further intrusion or damage and remove the cause of the problem. The action taken could require any of the following:
        (i) Disconnect or destroy affected system(s) or instances.
        (ii) Change passwords.
        (iii) Disconnect and disable user account(s).
        (iv) Block service ports or connections.
        (v) Block firewall ports or connections.
        (vi) Identify and, or disconnect IP addresses or intrusions.

3. Prevention: prevent reoccurrence
    A. Determine nature, origin, and source of occurrence or incident.
    B. Take steps to prevent reoccurrence (step 2, part B)
    C. Report event to Human Resources for evaluation and immediate enforcement of corrective action, punitive measures, or termination of employment.
    D. Plan training-awareness to make any new security issues known and mitigate any further damage.

Appendix B TDC CIS Systems: Maintenance Lifecycle and Purchasing Strategy

I. Business Continuity Challenge

1. Systems running past end of life cycle create down-time and loss of production and productivity in the following ways:
    a) Systems become unresponsive, slow and/ or simply stop working due to, but not limited to: (i) Hardware failure; and (ii) Inability to accommodate software changes or requirements: initiated by customers, vendor updates, or industry standards; including: (a) software update drivers, (b) hardware update drivers, (c) OS updates, patches, and service packs.
2. When the above occurs the following challenges are presented:
    b) Funding: resource allocation for replacement systems.
    c) Time: How to replace the systems in a timely manner.
    d) Response; Reactive vs. Proactive: emergency replacement systems put into place without planning. Emergency replacement systems do not provide maximum benefit. Lack of planning minimizes strategic potential of replacement systems.

II. Solution

1. Plan for expense and purchase, with a known price point, at regular intervals.
    a) Purchase predetermined minimum bare-bones replacement systems on set annual schedule*.
    b) New systems immediately built and put into production; replacing candidate system**.
    c) Candidate system criteria based on the following weighted factors:
        i. Age of system
        ii. Projected end of life
        iii. System's ability to perform designated purpose

* Predetermined minimum subject to change as per TDC CIS Systems environment dictates.
** Candidate system = System identified as reaching end of lifecycle

III. Benefit of approach

1. Planned budgeting for known expense and price-point alleviate portion of TDC CIS Systems expenditure strain on organizational bottom-line
2. Create a surplus and rotation of systems and replacement equipment and hardware, providing the following benefits:
    a) Help to plan systems replacement and upgrade schedule
    b) Minimize down-time and loss of productivity
    c) Facilitate a controlled environment for:
        i. Planned windows of down-time
        ii. Coordinate down-time around dependencies (interrelated systems)

III. Surplus, Rotation, and Re-purposing

1. End of life, or replaced systems, that are taken out of production will become either:
    a) Part of surplus to be parted out and re-purposed for other systems, and, or
    b) Immediately pushed down the line to replace/ rotated the next candidate system.

Appendix C TDC Disaster Recovery and Business Continuity

TDC Disaster Recovery and Business Continuity

Maintaining business continuity, and the security and confidentiality of our customers' data and property is our top priority. TDC is 100% HIPAA compliant and has over 18 years' experience in processing sensitive data and printing and handling critical documents.

Our processing facility is secured with electronic doors and key card system at all times. Authorized access to the production and processing area is limited to production staff and managers, company managers, and IT management. Any visitors/vendors that need access to our processing, facility are escorted by a company representative for paper deliveries and on-site shredding services.

Our Security system includes the following features:

- Outside Glass Detectors on all doors and windows
- Motion Detectors - internal and external
- Smoke Alarm System
- Sprinkler System
- Internal Camera System*
- Off Premises Camera Monitoring System
- Weekend and 3rd Shift Patrol

*All major traffic areas, entrance/ exits, hallways, production areas, are monitored via video surveillance on a 24hour, 7 days per week, and 365 days per year basis. All security cameras feed into a physically secure, central monitoring system capturing and retaining historical video feed for review of all facility activity as necessary.

The Data Center recognizes that it is imperative to have a back-up plan for any kind of emergency situation. We have developed plans for any such eventuality:

Power Failure and Fail Over: TDC maintains an industrial back-up generator to ensure continuity of business operations, despite power failure.

Site Resiliency and Fail Over: TDC SIA server farm is built upon an agile virtual platform, providing primary and secondary site fail-over and infrastructure services redundancy.

Equipment Issues: TDC houses redundant computer, printing, and mailing, equipment to ensure equipment failure will not inhibit production or jeopardize security. This redundancy includes our transportation vehicles as well.

Road Closure to Salt Lake City Bulk Mail Entry Unit USPS: TDC is within one mile of the SLC BMEU and has three alternate routes to get there. TDC holds permits at several other mail facilities so other locations could be used if necessary.

Communication: All key personnel have cellular phone service to be utilized in the event of POTS line failure. In addition our phone system is set up to forward to key personnel cell phones in case of emergency.

Disaster Recovery: In case of disaster, The Data Center has two plans for disaster recovery depending on whether the disaster is limited to our facility or if it incapacitates a larger geographical area.

Should disaster incapacitate our facility: TDC staff will be relocated to our disaster recovery facility to complete all daily required projects, scheduled printing and mailing. Our partner facilities have comparable capabilities, software, and equipment matching our own facility where DR transition will be transparent to our clients. Our advanced programming and our ability to create output in postscript lends itself to transition to either single or multiple facilities seamless. We have a disaster recovery drill with our partner facilities annually. If disaster incapacitates The Data Center and our confidential partner:
TDC facilitates getting our clients' secure data processed at one of over 20 of our confidential partner's facilities in the United States. We have an 'out of state' disaster recovery drill bi-annually.

Appendix D Risk Assessment: Impact Levels

1. TDC CIS SIA Categorization

The following tables represent the high-level and broad-spectrum overview of TDC SIA information types and information systems and the potential impact levels of each associated security objectives†.

1.2 Information Types Categorization*

Information Types Categorization				
Category	Description	Security Objective		
		Confidentiality	Integrity	Availability
TDC SIA: Customer Data	GVT	High	High	High
TDC SIA: Customer Data	PRI_1	High	High	High
TDC SIA: Customer Data	PRI_2	Low	High	Moderate
TDC SIA: Customer Data	PRI_3	Low	High	Moderate
TDC SIA: Data	ICD_1	Moderate	High	Moderate
TDC SIA: Data	ICD_2	Low	Low	Low
TDC SIA: Data	ICD_3	High	High	Moderate
TDC SIA: Data	ICD_4	High	High	Moderate

TDC Information Types

GVT = Government; all types will be regarded as high security objective

PRI = Private Sectors: 1 = Financial; 2 = Public; 3 = Administrative **

ICD = Internal Company Data: 1 = Financial; 2 = Public; 3 = Administrative; 4 = Information & Technology Management **

*Categorization for assessment purposes only. All TDC customer information will be considered confidential and handled as such.

** PRI information types: The three categories presented represent a broad-spectrum of possible private-sector information types only.

†Security objectives definitions found in Appendix D, section 1.4 TDC CIS Security Objectives.

1.3 Information Systems Categorization

Information Systems Categorization				
Category	Description	Security Objective		
		Confidentiality	Integrity	Availability
TDC SIA	External Customer-Facing Component	High	High	High
TDC SIA	Internal company-facing component	High	High	High

1.4 TDC CIS Security Objectives

The prescribed security objective and potential impact level definitions below are as shown in NIST, FIPS PUB 199; FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Standards for Security Categorization of Federal Information and Information Systems.

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]	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.
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 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES (NIST, 2004, pg. 6)

References

NIST. (2006). FIPS PUB 200, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Minimum Security Requirements for Federal Information and Information Systems March 2006. Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NIST. (2004). FIPS PUB 199, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Standards for Security Categorization of Federal Information and Information Systems February 2004. Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf