 FIRST THINGS FIRST <i>Ready for School. Set for Life.</i> Data Security Policy & Procedures	POLICY NO: IT - GENERAL 100	
	APPROVED BY: Rhian Evans Allvin	
Effective Date: 3/1/2010	Revision No: 3 (9/14/2011)	Page 1 of 8

BACKGROUND:

The purpose of First Things First (FTF) is to aid in the creation of a system that offers opportunities and supports for families and communities in the development of all children so they can grow up healthy and ready to succeed. Our work is accountable and transparent to decision-makers and the citizens of Arizona. To this end, First Things First collects and maintains data on the performance of its funded strategies as well as the early childhood system in Arizona.

AUTHORITY:

The Arizona Early Childhood Development and Health Board (AZECDH) shall develop, implement and maintain a coordinated Board plan for information technology (IT) (A.R.S. § 41-3504(A)(1)), including the formulation of policies to effectuate the purposes of the Board (A.R.S. § 41-3504(A)(13)).

PURPOSE:

The main objective of this policy is to ensure that data is protected in all its forms, during all phases of its life cycle, from inappropriate access, use, modification, disclosure, or destruction. Security compromises or access violations could threaten the security of the data and threaten the anonymity of individual or organizational data. Because data are a valuable asset to First Things First and the State of Arizona, this policy sets out guidelines for the security and integrity of data as well as guidelines for its distribution.

SCOPE:

This policy applies to First Things First staff as well as any other affiliate who is authorized to access data.

MAINTENANCE:

This policy will be reviewed by FTF Legal Counsel, the COO, and the Sr. Director of Research and re-approved by the CEO every 5 years or as deemed appropriate based on changes in technology or regulatory requirements.

ENFORCEMENT:

Violations of this Policy may result in suspension or loss of the violator’s use privilege. Additional administrative sanctions, civil, criminal, and equitable remedies may apply. (See Attachment A – Use of Electronic Equipment Policy and referenced IT Usage and Access personnel form).

EXCEPTIONS:

Exceptions to this policy must be reviewed by FTF’s Chief Executive Officer (CEO), under the guidance of the Legal Counsel.

DEFINITIONS:

Document: For purposes of this Policy, a Document is any printed hard-copy item that may contain Protected Information or data.

Data Media: For purposes of this Policy, Data Media is any magnetic, electronic or optical storage media item that may contain Protected Information or data.

Confidential Information: For purposes of this policy, Confidential Information means information other than Restricted Personal Identifying Information (RPII) that may only be disclosed as permitted or required by state or federal law or administrative rule. Confidential information includes critical business infrastructure information as defined by ARS 41-1801 and critical infrastructure information as defined by the U.S. Department of Homeland Security (6 USC 131; 49 CFR 1520).

POLICIES:

Throughout its lifecycle, all data shall be protected in a manner that is considered reasonable and appropriate for a public agency collecting program and quality improvement data. Any information system that stores, processes, or transmits data shall be secured in a manner that is considered reasonable and appropriate, as defined in FTF's IT Security Policy (Attachment B) approved by FTF's CEO and maintained by FTF's Chief Operating Officer (COO). Also see Physical Storage Security Policy and System Architecture and Secure Data Storage Policy located herein.

Individuals or institutions that are authorized to access data shall adhere to the appropriate roles and responsibilities, as defined in FTF Network Security Policy (Attachment C) approved by the CEO and maintained by the COO. All data and processing resources are only accessible on a least privilege basis to specifically identified, authenticated, and authorized users. User authentication and access shall be determined by the COO.

PUBLIC DATA POLICY:

FTF will provide access to aggregate statistical information that improves the early childhood-related decisions of providers, administrators, policymakers, parents, and other stakeholders. Confidential data on any individual will not be disseminated in violation of federal or state law. Furthermore, it shall not be used for any purpose other than those stated in this policy. If First Things First enters into a contract with a private individual or third party to collect data or perform any of the data reporting or statistical analysis, that agreement shall require that the data be protected in the same manner. First Things First will aggregate the data to comply with required state and federal reporting. Public data releases are reviewed by the COO or the Sr. Director of Research and Evaluation and authorized by CEO.

As well as having a duty to protect the information we hold, we are also required by the Arizona Public Records laws to make non-confidential information available to the public on request. In responding to requests from the public, we must ensure that sensitive information is not accidentally or inappropriately released, while at the same time meeting First Things First's obligations to disclose. Public information requests are reviewed by the Sr. Director of Communications and authorized by the CEO.

LIMITED DISTRIBUTION DATA POLICY:

First Things First recognizes the importance of availability of Arizona early childhood data to researchers. Through a formal request for publically available or limited use data, First Things First will work with researchers with the goal that they receive the most meaningful data possible without the disclosure of information that would make any participant's identity traceable. The request must explain the purpose of the research study, the facts that demonstrate that First Things First authorized the study or that the study is being conducted on behalf of First Things First, and how the researchers will ensure data confidentiality and security. A detailed Data Use Agreement will be signed by each researcher applying

for access to data. The Data Use Agreement will define the data covered by the agreement and will include how the data will be stored, accessed, used, maintained, disseminated and destroyed. Requests will be considered on a case-by-case basis by the CEO to determine if they are in compliance with state and federal laws and regulations.

Researchers will be required to supply a copy of any analysis or reports created with the data and to destroy the data once the research is completed. First Things First reserves the right to charge a reasonable fee for the use of data by researchers to help offset the state’s costs of collecting and storing the data.

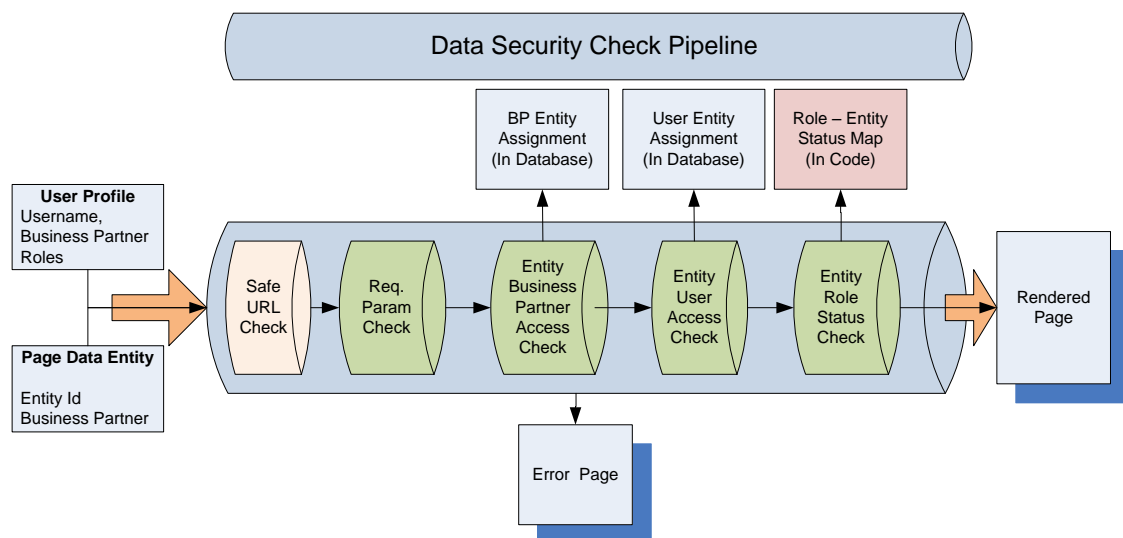
While it is anticipated that data containing personal identifiers would be shared only in very limited and extraordinary cases, in those instances any release of data to researchers outside First Things First is considered a loan of data, i.e., the recipients do not have ownership of the data. Prior to any data being shared, documentation and evidence of physical and process security standards meeting or exceeding that of FTF’s will be required, and the recipient of said data will be subject to onsite audits to verify this as being and remaining in place. At no time will a participant’s personal identifying information be sent via traditional mail, email, webmail, web browser, peer-to-peer network or via wireless transmission.

PARTNER DATA ACCESS POLICY:

While most information to be entered by partnering agencies and contained within the FTF system is deemed, by law and statute, as public information, certain information will only be available for viewing or manipulation by the individuals or organizations to whom that information pertains and those individuals or organizations identified as germane by FTF. The system interface may also be used to capture and communicate information relevant to monetary transactions. This information and its manipulation and the subsequent internal FTF functions will be secured to varying degrees so as to assure confidence of transactions. It is also necessary to secure that information from comprise where data and associated measures could influence future decisions of FTF, our Partners or other interested parties.

To achieve this objective, the FTF system will utilize a mechanism of authentication (identifying who they are) for those who come to the FTF site as well as authorization (identifying permissions and access levels). Both standard forms of authentication via user name and password and identity management are conducted using Active Directory. Figure 1 depicts FTF’s process which employs three checks for authentication and authorization of all users.

Figure 1: User Authentication and Authorization using Active Directory



PARTNERING EARLY CHILDHOOD AGENCIES:

In addition to end user access to our system in order to complete data input and/or financial transactions, First Things First (FTF) will capture and receive data from various agencies and through its own data collections systems for the purpose of longitudinal or other studies. FTF will also collect and store data regarding parents and children for the purpose of studies to determine if programs are successful and how to better serve the communities.

FTF will use sensitive or confidential data to produce aggregate reports. While it may seem that the use of anonymous aggregated data poses little threat to confidentiality, there are some cases where specific populations may include only a few individuals. Statistical disclosure is the risk that arises when a population is so narrowly defined that tabulations are apt to produce a reported number small enough to permit the identification of individuals. In such cases, the Sr. Director of Research and Evaluation will enforce statistical cutoff procedures using a minimum confidentiality. It is the intent of First Things to avoid any possibility of inadvertently reporting personally identifiable information.

CONFIDENTIAL DATA POLICY:

In capturing and receiving data, it may be necessary to collect HIPAA and FERPA regulated information for the purpose of matching individuals as individuals may also have interaction and data records with other agencies. HIPAA regulated information to be collected will consist, but not be limited to, data such as First Name, Last Name, Address with Zip Code, Date of Birth, and Social Security Number. This data is used for the purpose of identifying a child or parent to ensure it is the same individual(s) over time. These individual level data will be aggregated and integrated with information from other agencies to provide trend, usage and impact information over time. It is the intention of FTF to use this data only for matching populations and not report on it.

This data will be stored in a physically secured location and encryption procedures will be used to ensure data integrity and compliance with all the regulations for storing such data. Also see Physical Storage Security Policy/System Architecture and Secure Data Storage Policy located herein.

ACCESS TO CONFIDENTIAL DATA BY PERSONNEL:

To minimize the impact of any security violations and improve accountability, First Things First will provide staff with access to the minimum set of resources required for their role. Access to systems, applications, and information will only be granted in accordance with a formal, written, and auditable procedure (including a formal, written request for access to specific systems or data). FTF shall maintain a record of access to all data identified as limited use or confidential.

FTF's information technology (IT) personnel as well as other business units with necessary access to sensitive information are informed about the security policies and procedures for data identified as limited use or confidential. Practices such as separation of duties are utilized, when required and/or feasible, to ensure that personnel authorizing access to data are distinctly separate from those who can and are authorized to physically grant access. Whereas data management within FTF's database system is the responsibility of the Database Administrators, permission to access and/or to receive limited use or confidential data is authorized by the CEO and/or COO.

Because FTF's system will store limited use, confidential and HIPAA and/or FERPA regulated information, it is the policy of FTF to ensure compliance with rules and regulations. To ensure key staff is aware of the rules and regulations, as well as best practices when handling participant data, FTF requires staff that will have access to confidential data to complete the Federal NIH Collaborative Institutional Training

Initiative (CITI) Certification for training in human subject research and research ethics. Copy of this certification is recorded and on file with the COO.

DATA HANDLING POLICY:

Staff must ensure that all personal or sensitive information in their possession is kept secure at all times against unauthorized or unlawful loss or disclosure. It is the responsibility of staff to ensure that the following procedures are conducted.

- Paper files and other records or documents containing protectively marked/personal/sensitive information are kept in a secure physical environment;
- Protectively marked/personal/sensitive information held on computers and computer systems is stored in line with FTF data security policies;
- Protectively marked/personal/sensitive data is correctly secured if transmission of this type of data is necessary; and
- Protectively marked/personal/sensitive data is correctly disposed of, in line with data security policy.

At no such time will any identifying information be stored on portable devices (such as laptop computers, digital cameras, and portable hard drives including flash drives, USB memory sticks, iPods or similar storage devices). Any transport of data, including identifying information, must be conducted using secure, encrypted formats, ensuring user IDs are stored/transported separately.

Physical safeguards for workstations are practiced to restrict access to authorized users include the following.

1. All workstations are password protected.
2. Computer monitors are positioned so that visitors or unauthorized persons cannot easily view the screen or what is displayed.
3. Visitors are not allowed unsupervised access to areas where workstations with access to EHPI are housed.
4. Laptops are to be kept and not out of the control of employees who maintain and or have access to EHPI while outside the facility.
5. Laptops that are given to employees will be recorded and are the responsibility of that employee. If an employee's laptop is lost, damaged or stolen, it will be immediately reported to an administrator or their designee.

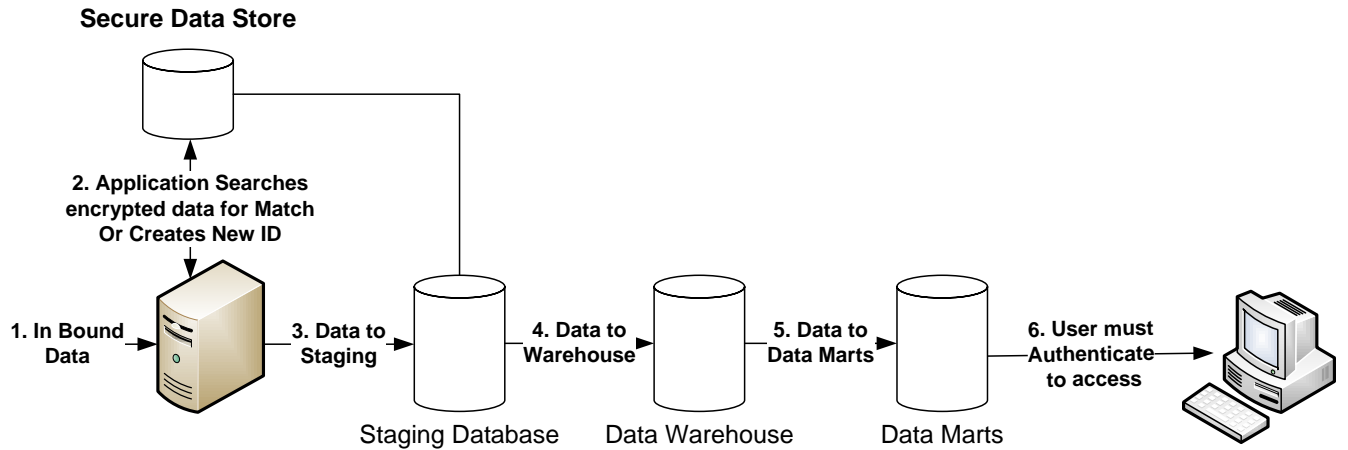
SYSTEM ARCHITECTURE AND SECURE DATA STORAGE POLICY:

First Things First will utilize a model to have separate storage of sensitive data and it will be encrypted. The surface storage and backups will be encrypted using Microsoft's SQL 2008 built-in functionality for creating certificates along with encryption and decryption functions to provide a secure solution. Field Level Encryption will be used, with encryption being done with certificates controlled by a separate group than FTF database administrators (DBAs).

All sensitive data will be stored in the Secure Data SQL file. It will be encrypted and stored as binary data type. User IDs are stored separate for those which encrypt and those that decrypt. Only those identified as a need to know and who are authorized will have access to said information. The keys for decryption will be encrypted as well and stored in a separate database from the actual data.

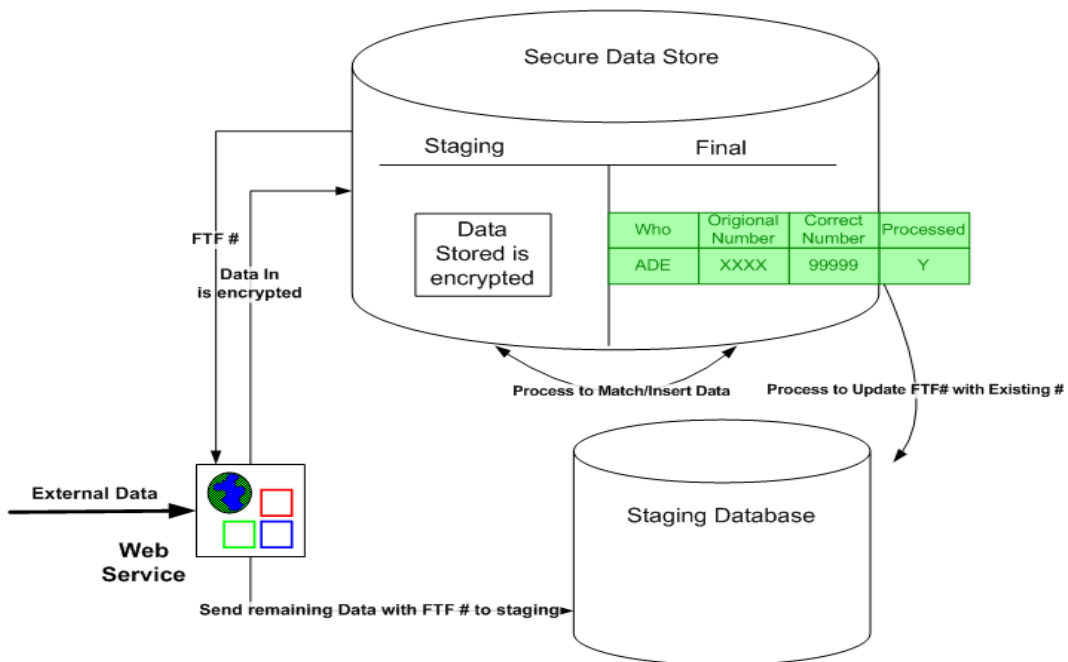
Figure 2 shows the High level architecture of the sensitive data model being used at First Things First.

Figure 2: Architecture of Secure Data Store



Sensitive Data will enter the system via two paths; externally through a secure web service and internally through the data collections built by FTF. Once the data is entered and requested to be saved, it will be sent to the Secure Data Store. Complete audit trails of every access will be recorded regardless of the user, for a complete audit trail. Transmitted data will not include any identifying information. Figure 3 provides an overview of FTF’s secure data storage and encryption process.

Figure 3: Secure Data Storage and Encryption Process



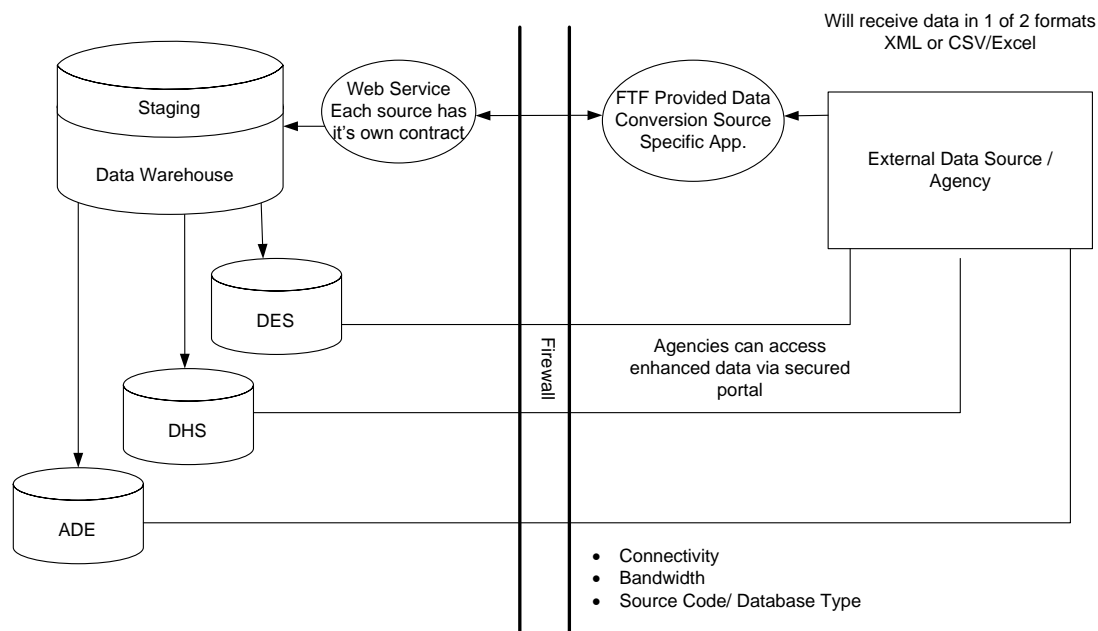
NETWORK ACCESS AND FIREWALL PROTECTION POLICY:

First Things First has a policy to securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

First Things First's network security standards provide secure and seamless interconnection of communications networks and systems while protecting FTF's physical and computing resources and data storage. Network security standards are employed through both FTF network infrastructure and the state's AZNET program for network communication services. Multi-layered protection is used at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into the FTF's information systems. External (inbound and outbound) traffic shall be routed through secure firewalls. Firewall technology utilized by FTF will have security logging employed. Individual firewalls deployed on FTF's systems are centrally administered and managed to ensure security is applied and updated.

FTF uses a web service, through standardized XML messaging or other formats, to receive, collect or exchange data with another web service. External connections to FTF networks shall be routed through secure gateways and protected by through encryption. Secure Socket Layer (SSL) is employed between a web server and browser to authenticate the web server and the user's browser. First Things First maintains an inventory of all external partners who have connections with FTF via a web service. FTF will promptly remove any external connections when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection. Figure 4 provides an example of external connections via secure gateway.

Figure 4: Secure gateway path for external connections



PHYSICAL STORAGE SECURITY POLICY:

First Things First will safeguard the physical housing unit of secure and protected data. The following physical security practices are followed.

- Information systems (servers, storage, client devices, etc.), media storage areas, and related communication wiring and network devices are located in secure locations that are locked and restricted to access by authorized FTF personnel only.
- Critical data or information storage areas are subject to access monitoring that establishes the identity of the person entering/exiting as well as the date and time of the access (e.g., recording badge information, videotaping) and provides data for auditing of physical access.
- Locking mechanisms with security ID badge or security ID badge and key access are used to access secure areas; access codes shall be changed periodically, according to a schedule defined by the budget unit.
- Where badge-reading systems are employed to log access into and out of a secure facility, “piggybacking” of badge holders shall be prohibited.
- Unused keys, entry devices, etc., shall be secured.
- Physical access to “critical” IT hardware, wiring, and network devices shall be controlled for access by restricted/minimal privilege necessary for the authorized employee or contractor to complete assigned tasks.
- Physical access security measures employed for back-up systems/servers shall be equivalent to those of the primary system.
- Information systems, media storage areas, and related communication wiring and network devices should be protected against loss or malfunction of environmental equipment or services necessary for the operation of the facility.

Because theft or loss of IT equipment may potentially result in the unintentional disclosure of confidential information, FTF’s computing and telecommunications equipment is password protected and routinely inventoried, accounted for, and safeguarded from loss and resulting unauthorized use. Removable storage media (disk, tapes, CDs, etc.) are consistently controlled and labeled to guard against misplacement and loss or unauthorized use of information.

POLICY FOR CASE OF BREACH:


An important aspect of First Things First data security policies is the effective and timely reporting of all suspected incidents of misuse or loss of protectively marked/ personal/sensitive information or breaches of data security. FTF will promptly identify, manage, report, manage and provide notification of a data breach related to an information security incident.

In the event a security breach occurs the following steps should be followed:

1. Data Systems identified should be shut down immediately and taken off the network.
2. The extent of the data accessed should be identified.
3. The IT Director should be notified immediately of the breach and the extent of the breach.
4. The Arizona Department of Administration’s Arizona Strategic Enterprise Technology Office (ASET) a must be notified within 1 hour of breach.
5. IT Director will work with the CEO, COO, and Communications Director to come up with a communication plan to release if deemed necessary.
6. All individuals or the guardians of individuals whose data was breached must be notified.
7. Any suspect component of the IT infrastructure must be clean and secure before bringing the component back on line.

Attachments:

- A. Use of Electronic Equipment Policy and Personnel Form
- B. FTF IT Security Policy
- C. FTF Network Security Policy

 Use of Electronic Equipment	POLICY NO: IT - GENERAL 100	
	APPROVED BY: Rhian Evans Allvin	
Effective Date: 8/10/2008	Revision No: 3 (4/12/2011)	Page 10 of 3

- **AUTHORITY**

The Arizona Early Childhood Development and Health Board (AZECDH) shall develop, implement and maintain a coordinated Board plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including the formulation of policies to effectuate the purposes of the Board (A.R.S. § 41-3504(A (13))).

- **PURPOSE**

The purpose is to establish a Board policy for proper Internet/ Intranet use and to require State employees and contractors to be informed of acceptable and unacceptable uses of State equipment before accessing the Internet/ Intranet.

- **SCOPE**

This applies to all divisions within AZECDH.

The Board Chief Executive Officer, working in conjunction with the Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each Division.

- **POLICY**

Employees may be assigned computer equipment, a telephone with voice mail, and a Blackberry or cell phone. Additionally, they have access to printers, fax machines, scanners, and other electronic means of communications or data processing. Employees using the Share Point Intranet will develop professional business sites that reflect the mission of the Board. The following activities are prohibited on the First Things First electronic equipment:

Attachment A

- The unauthorized modification or destruction of data or software.
- The intentional creation of misleading or unauthorized records or data.
- Communications by means of electronic equipment which are harassing or offensive to another.
- The possession or transmission of sexually explicit or pornographic material.
- The storage, use or transmission of personal software, files or data unless such software, files, or data is work related and has been approved in writing by the COO.
- Authorized equipment is the property of State government. Under no circumstances should authorized equipment be used for personal use. If an employee requires use of their assigned equipment for personal use, employee should notify direct supervisor.
- The unauthorized access to another employee's computer or telephone.
- The unauthorized use or release of passwords.
- Playing computer/ PDA games during work hours.
- Recording meetings or conversations without prior consent of all participants of the meeting or conversation. This does not apply to investigations authorized by the CEO or COO.
- **REFERENCES**
 - A. R. S. § 41-3504, "Powers and Duties of the Agency."
- **ATTACHMENTS**
 - Attachment A. Sample Internet User Consent Form

ATTACHMENT A: USE OF ELECTRONIC EQUIPMENT CONSENT FORM

_____ **Electronic Equipment User Consent**


I, _____, have read and understand the Statewide Use of Electronic Equipment Policy. I agree to comply with all of the terms and conditions of this policy. I understand and agree that my employer reserves the right to monitor and log all network and Internet activity, including email, without notice. I have no expectation of privacy in the use of these resources. Further, I understand and agree that all network and information systems activity conducted with State/Agency resources is the property of the State of Arizona.

Signed: _____

Date: _____

LIABILITY

Neither the State of Arizona nor the _____ (Agency Name) make warranties of any kind, whether express or implied, for the use of the email system or electronic information resources. Additionally, neither the State of Arizona nor the agency indicated above is responsible for any damages, whatsoever, that employees, may suffer arising from or related to the use of Internet resources.

 FIRST THINGS FIRST <i>The right system for bright futures</i> IT Security Policy	POLICY NO: IT - GENERAL 100	
	APPROVED BY: Rhian Evans Allvin	
Effective Date: 10/10/2008	Revision No: 3 (3/10/2010)	Page 13 of 5

1. AUTHORITY

The Arizona Early Childhood Development and Health Board shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including adopting statewide technical, coordination, and IT policy and standards (A.R.S. § 41-3504(A (1(a))))).

2. PURPOSE

To establish a Board security policy for the protection of IT assets and resources, including data/information with our own network infrastructure and the AZNET program for network services.

3. SCOPE

This applies to all divisions within the Board.

The Chief Executive Officer working in conjunction with the Chief Information Officer (CIO) shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each Division.

4 POLICY

The State of Arizona shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

4.1 IT SECURITY POLICY RESPONSIBILITIES

The policy establishes that the Board shall:

- 4.1.1 Protect the State’s IT assets, resources, and data/information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
 - Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

- Confidentiality, which means preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
 - Availability, which means ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, authorization and access control;
 - Accountability, which includes requirements that actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures; and
 - Assurance, including security administration and adherence to Statewide IT security policies and standards.
- 4.1.2 Provide security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either information collected or maintained by or on behalf of the Board.
- 4.1.3 Ensure that data/information contained in electronic transactions is protected via 1) identification, authentication, and authorization; 2) encryption; and 3) electronic signature, as necessary.
- 4.1.4 Provide adequate security for all information collected, processed, transmitted, stored, or disseminated in the Division’s software application systems.
- 4.1.5 Ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, using cost-effective management, personnel, operational, and technical controls.
- 4.1.6 Apply security controls to information systems, resources, and data/information sufficient to contain risk of loss or misuse of the information to an acceptable level that supports the mission and operation of the Board.
- 4.1.7 Ensure that information security management processes are integrated with the Board’s strategic and operational planning processes, including planning and implementing (see paragraph 4.6) any necessary remedial action to address IT security deficiencies.
- 4.1.8 Communicate applicable Statewide and IT security policies and standards to appropriate third-party organizations.
- 4.1.9 Establish IT security programs, including assignment of roles and responsibilities, as well as creation of any necessary procedures, adherence requirements, and monitoring controls that adhere to:
- *Statewide Policy P800, IT Security*;
 - Applicable Statewide Standards for IT security; and
 - Budget-unit-specific IT security policies, standards, and procedures.

- Budget unit IT security programs shall be appropriate to each budget unit’s operational and technology environment in order to provide a foundation for management to make informed decisions and IT investments that appropriately mitigate IT security risks to an acceptable level.

4.2. SECURITY ARCHITECTURE STANDARDS

Security Architecture defines common, industry-wide, open-standards-based technologies required to enable secure and efficient transaction of business, delivery of services, and communications among its citizens, the federal government, cities, counties, and local governments, as well as the private business sector. Security Architecture Standards allow the State and individual budget units to quickly respond to changes in technology, business, and information requirements without compromising the security, integrity, and performance of the enterprise and its information resources. Refer to Paragraph 6.20, Statewide Standards for Security Architecture, for further information.

4.3. IMPLEMENTATION

Arizona’s EWTA has been designed to maximize current investments in technology, provide a workable transition path to targeted technologies, maintain flexibility, and to enhance interoperability and sharing. Security Architecture implementations shall adhere to implementation strategies described in *Statewide Policy P700, Enterprise Architecture*. Security Architecture shall be implemented in accordance with this policy, applicable statewide standards for security, and relevant Federal, and individual budget unit standards.

4.6. CONFORMANCE OF IT INVESTMENTS AND PROJECTS TO EA

To achieve the benefits of an enterprise-standards-based architecture, all information technology investments shall conform to the established EWTA that is designed to ensure the integrity and interoperability of information technologies for budget units. *Statewide Standard P340-S340, Project Investment Justification (PIJ)*, defines conformance with the established EWTA and associated Statewide Policies and Standards. Variances from the established EWTA shall be documented and justified in the appropriate section of the PIJ document.

4.7. APPLICABILITY TO OTHER STATEWIDE EA POLICIES AND STANDARDS

Statewide Policy P800, IT Security, adheres to and demonstrates the purpose established in *Statewide Policy P100, Information Technology*. *Statewide Policy P800, IT Security*, adheres to the principles, governance, lifecycle

process, and implementation elements described in *Statewide Policy P700, Enterprise Architecture*.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at

http://www.azgita.gov/policies_standards/ for definitions and abbreviations.


6. REFERENCES

- 6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.4. A. R. S. § 41-1461, “Definitions.”
- 6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.8. A. R. S. § 41-3501, “Definitions.”
- 6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 6.15. Federal Office of Management and Budget (OMB) Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources.”
- 6.16. State of Arizona Target Security Architecture.
- 6.17. [Statewide Policy P100, Information Technology](#).
- 6.18. [Statewide Policy P340, Project Investment Justification \(PIJ\)](#).
 - 6.18.1. [Statewide Standard P340-S340, Project Investment Justification](#).
- 6.19. [Statewide Policy P700, Enterprise Architecture](#).
- 6.20. [Statewide Policy P800, IT Security](#).
 - 6.20.1. [Statewide Standard P800-S805, IT Risk Management](#).
 - 6.20.2. [Statewide Standard P800-S810, Account Management](#).
 - 6.20.3. [Statewide Standard P800-S815, Configuration Management](#).
 - 6.20.4. [Statewide Standard P800-S820, Authentication and Directory Services](#).
 - 6.20.5. [Statewide Standard P800-S825, Session Controls](#).
 - 6.20.6. [Statewide Standard P800-S830, Network Infrastructure](#).
 - 6.20.7. [Statewide Standard P800-S850, Encryption Technologies](#).
 - 6.20.8. [Statewide Standard P800-S855, Incident Response and Reporting](#).
 - 6.20.9. [Statewide Standard P800-S860, Virus and Malicious Code Protection](#).

- 6.20.10. [Statewide Standard P800-S865, IT Disaster Recovery Planning \(DRP\).](#)
- 6.20.11. [Statewide Standard P800-S870, Backups.](#)
- 6.20.12. [Statewide Standard P800-S875, Maintenance.](#)
- 6.20.13. [Statewide Standard P800-S880, Media Sanitizing/Disposal.](#)
- 6.20.14. [Statewide Standard P800-S885, IT Physical Security.](#)
- 6.20.15. [Statewide Standard P800-S890, Personnel Security.](#)
- 6.20.16. [Statewide Standard P800-S895, Security Training and Awareness.](#)

7. ATTACHMENTS

None.

 FIRST THINGS FIRST <i>The right system for bright futures</i> Network Security Policy	POLICY NO: IT-GENERAL 100	
	APPROVED BY: Rhian Evans Allvin	
Effective Date: 10/10/2008	Revision No: 3 (3/10/2010)	Page 18 of 7

1. AUTHORITY

The Arizona Early Childhood Development and Health Board shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a))))).

2. PURPOSE

To establish a Board policy to provide for secure and seamless interconnections of the Board’s heterogeneous systems and communications networks, including wireless, modems, routers, switches, and firewalls and protecting the Board’s computing resources and information from the risk of unauthorized access from external sources.

3. SCOPE

This applies to all divisions within the Board.

The Chief Executive Officer working in conjunction with the Chief Information Officer (CIO) shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each Division.

4. Policy

The State of Arizona security standards shall be used to provide the minimum requirements for providing secure and seamless interconnection of communications networks and systems while protecting the State’s computing resources and information whether that is through existing Board network infrastructure or through the states AZNET program for network communication services. Multi-layered protection shall be deployed at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into the State’s information systems.

4.1. NETWORK PERIMETER SECURITY:

The policy establishes that the Board shall:

- 4.1.1. Employ firewall technology at the edge of a Board's network including the Internet Gateway, to protect sensitive internal information assets and infrastructure from unauthorized access. External (inbound and outbound) traffic shall be routed through secure gateways, such as firewalls.
- 4.1.1 Establish network traffic filtering rules for traffic that traverses the Internet shall include the following:
 - An incoming packet shall not have a source address of the internal network,
 - An incoming packet shall not contain Internet Control Message Protocol (ICMP) traffic,
 - An incoming packet shall have a publicly registered destination address associated with the internal network if using static or dynamic Network Address Translation (NAT),
 - An incoming packet should not contain Simple Network Management Protocol (SNMP) traffic,
 - An outgoing packet shall have a source address of the internal network,
 - An outgoing packet shall not have a destination address of the internal network,
 - An incoming or outgoing packet shall not have a source or destination address that is private or listed in RFC 1918-reserved space,
 - Sources of traffic from Internet sites that are known to contain spam, offensive material, etc., may be blocked at the discretion of the Board.
- 4.1.2 Block inbound or outbound traffic containing source or destination addresses of 127.0.0.1 or 0.0.0.0, or directed broadcast addresses.
- 4.1.3 The Board may collectively establish inter-agency service agreements (ISAs) to implement and maintain a "trusted peer" relationship among multiple participants. Each participant in the agreement shall agree to conform to all applicable requirements set forth in the agreement to ensure sufficient and acceptable security protection for all other participating entities.
- 4.1.10 Establish IT network security programs, including assignment of roles and responsibilities, as well as creation of any necessary procedures, adherence requirements, and monitoring controls that adhere to:
 - *Statewide Policy P800-S830, Network Security*;
 - Applicable Statewide Standards for network security; and
 - Board-specific IT security policies, standards, and procedures.

- 4.2. **END POINT SECURITY:** Client platform devices, including Board-owned assets, client devices used by remote workers and telecommuters, as well as third-party entities, connected to the Board's internal network should be protected from sending or receiving hostile threats from unauthorized network traffic or software applications.
- 4.2.1 Client platform devices shall utilize virus-scanning software in accordance with *Statewide Standard P800-S860, Virus and Malicious Code Protection*.
 - 4.2.2 Client platform devices externally connecting to Board internal networks shall encrypt all traffic in accordance with paragraph 4.6.
 - 4.2.3 Individual firewalls deployed on client platform devices provide protection against network-borne threats by providing traditional firewall services blocking network traffic based on protocol, ports, and software applications, content filtering of packets, as well as controlling the behavior of software applications deployed and executed on the client platform device.
- 4.3. **ACCESS TO INTERNETWORKING DEVICES AND SHARED PLATFORMS:** Internetworking devices (including routers, firewalls, switches, etc.) and shared platforms (including mainframes, servers, etc.) provide both access to and information about networks. They shall be controlled to prevent unauthorized access.
- 4.3.1 Access to Internetworking devices and shared platforms shall be restricted to authorized employees and contractors in accordance with *Statewide Standard P800-S885, Physical Security*, and *Statewide Standard P800-S875, Maintenance*.
 - 4.3.2 Access to network management tools such as Simple Network Management Protocol (SNMP), Secure Socket Shell (SSH), and Remote Monitoring (RMON), etc., as well as telnet access, shall be controlled. SNMP shall be version 3 or higher to take advantage of improved security features.
 - 4.3.3 Internetworking devices connected to the Internet shall have RFC 1918 and RFC 2827 implemented for inbound traffic.
 - 4.3.4 Internetworking device passwords shall be immediately changed before or upon device installation and shall conform to requirements set forth in *Statewide Standard P800-S820, Authentication and Directory Services*, and Board specific password criteria.
 - 4.3.5 Internetworking devices shall be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process.
 - 4.3.6 When disposing of internetworking devices that are no longer used by the Board, all configuration information shall be cleared in accordance with *Statewide Standard P800-S880, Media*

Sanitizing/Disposal, to prevent disclosure of network configuration, keys, passwords, etc.

- 4.4. **PATCH MANAGEMENT**: The Board shall develop and implement written procedures that identify roles and responsibilities for implementing patch management that include the following activities:
 - 4.4.1 Authorized Board employees or contractors shall proactively monitor and address software vulnerabilities of all internetworking devices in their network (routers, firewalls, switches, etc) by ensuring that applicable patches are acquired, tested, and installed in a timely manner.
 - 4.4.2 Where practical and feasible, the Board designated staff shall test patches in a test environment prior to installing the patch.
 - 4.4.3 Patches shall be installed on all affected internetworking devices. Designated employees or contractors shall monitor the status of patches once they are deployed.
 - 4.4.4 Patches make changes to the configuration of an internetworking device designed to protect and secure internetworking devices and attached IT devices and systems from attack, and shall be controlled and documented in accordance with *Statewide Standard P800-S815, Configuration Management*.
- 4.5. **DEMILITARIZED ZONE**: Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, VoIP, etc.) shall be deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ.
 - 4.5.1 All communication from servers on the DMZ to internal applications and services shall be controlled.
 - 4.5.2 Remote or dial-in access to networks shall be authenticated at the firewall, or through services placed on the DMZ.
 - 4.5.3 The DMZ is the appropriate location for web servers, external DNS servers, Virtual Private Networks (VPNs), and dial-in servers.
 - 4.5.4 Any Board external DNS servers should neither be primary servers nor permit zone transfers to DNS servers outside of the Board.
 - 4.5.5 All remote access users shall be considered external and therefore should be subjected to the firewall rule set. VPNs should terminate on the external segment or outside of the firewall.
- 4.6. **EXTERNAL CONNECTION TO NETWORKS**: External connections to networks shall be routed through secure gateways and protected by the following encryption methods, as appropriate:
 - 4.6.1 At a minimum either Triple DES (TDES) or Advanced Encryption Standard (AES) shall be deployed and supported for the transmission of

data/information as identified in the *Statewide Standard, P800-S850 Encryption Technologies*.

- 4.6.2 Transport Layer Security (TLS) or Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementations of TLS and SSL shall allow for client authentication support using the services provided by Certificate Authorities.
 - 4.6.3 Wireless Transaction Layer Security (WTLS) with strong authentication and encryption shall be used between a web server and the browser of a wireless mobile device, such as a cellular telephone, PDA, etc., to provide sufficient levels of security during data transmission.
 - 4.6.4 VPNs shall be used to connect two networks or trading partners that must communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using a version of the IPSec security protocol.
 - 4.6.5 Strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, shall be used once permission to connect has been granted.
 - 4.6.6 External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.
- 4.7. **INTER-NETWORK TRANSPORT SERVICES:** Based on the Board's business requirements, inter-network transport services are configured and implemented to allow for automatic re-routing of communications when critical nodes or links fail, or fall-back to alternate transport services, including the provision of duplicate or alternate secure gateways and external exchanges or switching centers.
- 4.8. **WIRELESS NETWORK ACCESS:** The Board shall ensure that centralized user authentication in accordance with *Statewide Standard P800-S820, Authentication and Directory Services*, encryption technologies with automated key distribution, and VPN technologies are used as appropriate with standard wireless networks: IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).
- 4.9. **INTRUSION DETECTION/PREVENTION:** The Board shall ensure detection mechanisms or intrusion prevention tools are incorporated into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments.
- 4.9.1 When used, intrusion detection systems shall be installed both external and internal to firewall technology protecting the network to monitor, block, and report unauthorized activity.

- 4.9.2 Intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.
 - 4.9.3 Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been misconfigured.
 - 4.9.4 Violations of set parameters shall trigger appropriate notification to security administrators or Board staff, allowing a response to be undertaken.
 - 4.9.5 When manufacturer recommended updates/patches are applied to IDS/IPS systems that may impact end-user connectivity, notification to all impacted entities/users as to date and time shall occur prior to any updates.
- 4.10. **VULNERABILITY SCANNING:** Network and host vulnerability scanners shall be used to test for the vulnerabilities of internal systems and of network perimeter defenses, as well as adherence to security policy and standards.
- 4.11. **DESTRUCTION OF NETWORK DOCUMENTATION:**
 Destruction of hardcopy and electronic documentation of network device configurations, network diagrams, etc., shall be destroyed, when superseded, or no longer needed. Such destruction may be completed on-site by the use of a commercial strength document shredder and/or the use of a secure recycling container.

5. **DEFINITIONS AND ABBREVIATIONS**

Refer to the PSP Glossary of Terms located on the GITA website at

http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. **REFERENCES**

- 6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.4. A. R. S. § 41-1461, “Definitions.”
- 6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.8. A. R. S. § 41-3501, “Definitions.”
- 6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”

- 6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 6.15. [Statewide Policy P100, Information Technology.](#)
- 6.16. [Statewide Policy P710, Network Architecture.](#)
 - 6.16.1. [Statewide Standard P710-S710, Network Infrastructure.](#)
- 6.17. [Statewide Policy P800, IT Security.](#)
 - 6.17.1. [Statewide Standard P800-S815, Configuration Management.](#)
 - 6.17.2. [Statewide Standard P800-S820, Authentication and Directory Services.](#)
 - 6.17.3. [Statewide Standard P800-S850, Encryption Technologies.](#)
 - 6.17.4. [Statewide Standard P800-S860, Virus and Malicious Code Protection.](#)
 - 6.17.5. [Statewide Standard P800-S875, Maintenance.](#)
 - 6.17.6. [Statewide Standard P800-S880, Media Sanitizing/Disposal.](#)
 - 6.17.7. [Statewide Standard P800-S885, IT Physical Security.](#)
- 6.18. State of Arizona Target Security Architecture,
http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.