First Things First
Data Security Policy & Procedures

BACKGROUND:
The purpose of the Arizona Early Childhood Development and Health Board (First Things First - FTF) is to aid in the creation of a system that offers opportunities and support 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, FTF collects and maintains data on the performance of its funded strategies as well as the early childhood system in Arizona.

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 is a valuable asset to FTF 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 FTF staff as well as any other individual or entity that is authorized to access the data.

DEFINITIONS:
Public Data: Public data is data that is readily available in the public sphere, such as websites, publications, or other widely used sources. Public data includes both data published by FTF (e.g., needs and assets reports and impact reports) and data that has been officially released by an organization and is able to be located and verified by any interested party utilizing the complete citation (e.g., census data). Public data also includes aggregated data, except where the aggregated data constitutes limited distribution data.

Limited Distribution Data: Limited distribution data is aggregated data that does not identify individuals, but which may be of sufficiently small cell size (e.g., less than 10) that its dissemination poses a reasonable risk to the anonymity of any individual. FTF's Data Suppression guidelines contain statistical cutoff procedures to help ensure that limited distribution data does not put at risk the anonymity of any individual. FTF's intent is to avoid the possibility of inadvertently reporting personally identifiable information. Limited distribution data may be subject to HIPAA, FERPA, tribal law, or other data regulation. (For the purposes of ADOA-ASET Policy 8110, limited distribution data is a form of confidential data.)

Confidential Data: Confidential data is non-public data that identifies individuals or is governed by agreements or laws that limit its viewing, analysis, or dissemination. Confidential data may also include confidential business information. Confidential data may be subject to HIPAA, FERPA, tribal law, or other data regulation. *See also* ADOA-ASET Policy 8110 ¶ 6.2.1. (ADOA-ASET defined confidential data, sensitive data and sensitive information are all forms of confidential data for the purposes of this Policy.)

POLICY:
FTF captures and receives data from various agencies and through its own data collections systems for the purpose of longitudinal or other studies. FTF also collects and stores data regarding children and families for the purpose of evaluating if FTF-funded programs and services are successful and how to better serve communities (e.g., needs and assets reports).

Throughout its lifecycle, data and any information system that stores, processes, or transmits data will be protected and secured in a manner that is considered reasonable and appropriate for a public agency collecting program, quality improvement, and research data. Details about physical storage and encryption procedures are described below under the headings "Physical Storage Security" and "System Architecture and Secure Data Storage."

All information systems containing non-public data or processing resources will only be accessible on a least privilege basis to specifically identified, authenticated, and authorized users. User authentication and access will be determined by the COO. FTF employees will also be required to sign the State's information technology Access Agreement (Attachment A).

FTF will not publish or otherwise disseminate confidential data in violation of law. Furthermore, confidential data will not be disseminated for any purpose other than those stated in this policy. If FTF enters into a contract with a third-party to collect data or perform data reporting or statistical analysis, that contract will require the third-party to protect confidential data as well. *See Data Security, Submission and Suppression Guidelines and Requirements for Collaborators*.

AGGREGRATED DATA:

FTF uses confidential data to produce aggregate reports. In general, this aggregated data will be public data. In some cases, however, specific populations include only a few individuals. This creates a risk that even aggregated data for those populations will permit the identification of individuals. In those cases, the aggregated data for those populations becomes limited distribution data. This aggregated limited distribution data will be suppressed in publications in accordance with FTF's Data Suppression guidelines. This limited distribution data may also be suppressed or protected by contract in other disclosures.

HIPAA & FERPA:

FTF sometimes receives or collects information covered by HIPAA or FERPA. HIPAA and FERPA protected information may include data such as First Name, Last Name, Address with Zip Code, Date of Birth, and Social Security Number. FTF will protect HIPAA and FERPA protected data as required by those laws.

Sometimes HIPAA and FERPA protected data is used for the purpose of identifying a child or parent to ensure it is the same individual(s) over time. This individual-level data will be aggregated and integrated with information from other agencies to provide trend, usage and impact information over time. FTF's intention is to use this personally identifying information to match data sets to individuals and not to report on the personally identifying information.

Data protected by HIPAA, FERPA or any other law will not be shared with the public, researchers, partners or tribes unless permitted by that law.

PUBLIC ACCESS TO DATA:

FTF will provide the public with access to public data, following a request, in accordance with Arizona's Public Records Laws. The COO or the Sr. Director of Research and Evaluation will review the data before disclosure to the public to ensure that non-public data is not accidentally or inappropriately released.

RESEARCHER ACCESS TO DATA:

FTF recognizes the importance of availability of Arizona early childhood data to researchers. When researchers request access to limited distribution or confidential data, FTF will work with the researchers with the goal that they will receive the most meaningful data possible while ensuring that

information will not be disclosed to the public that could be used to identify individuals to whom the data relates. FTF will also work to ensure that researchers do not misuse data by drawing and publishing conclusions not supported by the data or by using data contrary to the conditions that were placed on FTF's ability to collect and use the data.

Researchers' request for access to confidential or limited distribution data must explain the purpose of the research study; identify any facts, if applicable, that demonstrate that FTF authorized the study or that the study is being conducted on behalf of FTF; and explain how they will ensure data confidentiality and security. Each researcher will be required to sign a detailed data use agreement before receiving access to the data. The data use agreement will define the data covered by the Agreement and will set out how the data will be stored, accessed, used, maintained, disseminated and destroyed. Researchers will also be required to supply FTF with a copy of any analysis or report created with the data and to destroy their copies of the data once the research is completed. Researchers' requests will be considered on a case-by-case basis.

It is anticipated that data containing personal identifiers will be shared with researchers only in very limited cases. In those instances, any release of data to researchers will be considered a loan of data; i.e., the recipients will not have ownership of the data. Prior to data containing personal identifiers being shared, FTF will require documentation and evidence of the researchers' physical and process security standards meeting or exceeding that of FTF's, and the researchers will be subject to onsite audits by FTF to verify these standards as being and remaining in place. FTF will not send a service recipient or research participant's personal identifying information via email, webmail, web browser, peer-to-peer network or wireless transmission; the preferred method of transmittal is through an established secure web service or secure FTP (File Transfer Protocol) site via the internet.

PARTNER ACCESS TO DATA:

Most data contained within the FTF system that has been shared or entered directly by partnering agencies and entities will be public data. But certain data from partnering agencies will only be available for viewing or manipulation by FTF, the individuals, agencies or entities to whom that data pertains, and those individuals, agencies or entities identified as germane by FTF.

FTF may share personally identifying information with another government agency when that information is necessary to link data held by FTF to data held by the other agency. Additionally, where FTF is one of multiple partnering agencies and entities jointly working on a specific project, then FTF may share confidential data collected as part of the project with the other partnering agencies and entities.

TRIBAL ACCESS TO DATA:

Tribes may have access to data collected from children and families living on their tribal lands in accordance with FTF's Tribal Data Policy.

FINANCIAL DATA:

FTF's 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 compromise where data and associated measures could influence future decisions of FTF, its Partners, or other interested parties.

DATA SUPPRESSION:

Confidential and limited distribution data must not appear in publications. When a publication includes aggregate data, any limited distributed data must be suppressed. The statistical cutoff procedures help ensure that aggregated data does not put at risk the anonymity of any individual. FTF's intent is to avoid the possibility of inadvertently reporting personally identifiable information.

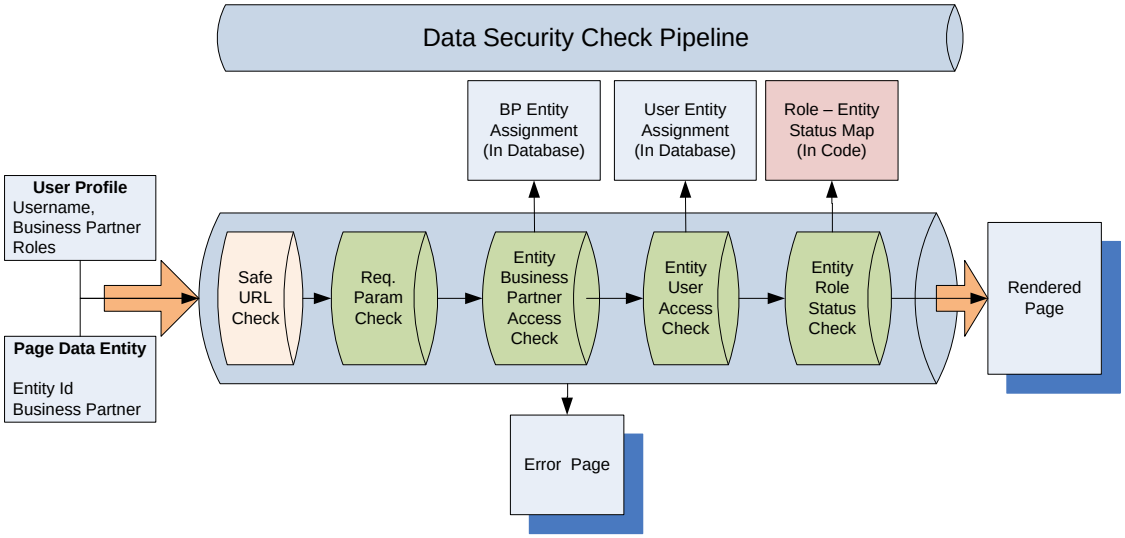
For data related to social service and early education programming, limited distribution data refers to counts of fewer than ten, excluding counts of zero (i.e., all counts of one through nine). Examples of social service and early education programming include the number of children served in TANF, AzMerit scores, and the number of children served with an IEP.

For data related to health or developmental delay, limited distribution data refers to counts of fewer than six, excluding counts of zero (i.e., all counts of one through five). Examples of health or developmental delay include the number of children without health insurance and the number of newborns admitted to an ICU.

USER AUTHENTICATION AND AUTHORIZATION:

In order to provide partnering agencies with limited access to shared data and certain financial information, 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 authorization via 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



STAFF ACCESS TO DATA:

To minimize the impact of any security violations and improve accountability, FTF provides staff with access only to the minimum set of data resources required for their role. FTF will maintain a record of electronic access to all data identified as limited distribution or confidential.

FTF's information technology (IT) personnel as well as other business units with necessary access to confidential data are informed about the security policies and procedures for data identified as limited

distribution 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. The CEO or COO may authorize access to limited distribution and confidential data, and database administrators grant physical access.

Because FTF's system will store limited distribution and confidential data, including HIPAA and/or FERPA regulated information, FTF wants to ensure compliance with applicable rules and regulations. To ensure key staff is aware of the rules and regulations, as well as best practices when handing participant data, FTF requires staff that will have electronic access to confidential data to complete the Federal NIH Collaborative Institutional Training Initiative (CITI) Certification for training in human subject research and research ethics. A copy of this certification is recorded and placed on file with the COO.

DATA HANDLING:

Staff must ensure that all confidential data 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 physical records or documents containing confidential data are kept in a secure physical environment;
- Confidential data held on computers and computer systems is stored in line with FTF data security policies;
- Confidential data being hand-carried is kept with an authorized staff member and protected from unauthorized disclosure;
- Confidential data is not left unattended, even temporarily, outside of a controlled area or an authorized employee's physical control;
- Confidential data is not moved without authorization outside of a controlled area or an authorized employee's physical control;
- Confidential data is not discussed in the presence of unauthorized individuals;
- Confidential data is turned over or put out of sight when individuals not authorized to view the data are present;
- Confidential data is correctly secured if transmission of this type of data is necessary; and
- Confidential data is correctly disposed of, in line with this policy.

Staff must not store collected data with identifying information on portable devices (such as laptop computers, digital cameras, tablets, smartphones, and portable hard drives including flash drives, USB memory sticks, or similar storage devices). Any transmission of confidential or limited distribution data, including identifying information, must be conducted using secure, encrypted formats, ensuring user IDs are stored/transported separately.

FTF practices physical safeguards for workstations to restrict access to authorized users, including 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 electronic health protected information are housed.
4. Employees who maintain and/or have access to electronic health protected information must keep their laptops within their control 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 must be immediately reported to an administrator or their designee.

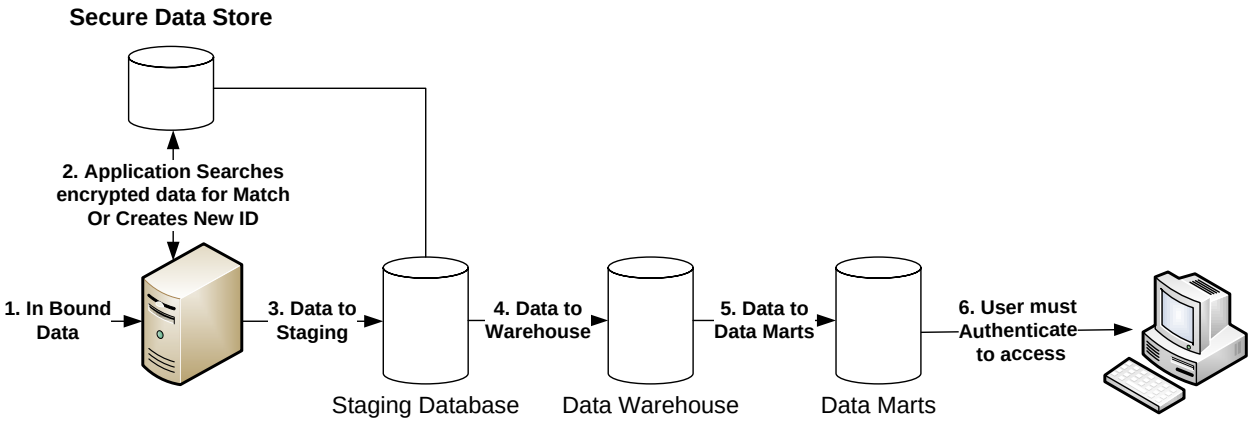
SYSTEM ARCHITECTURE AND SECURE DATA STORAGE:

FTF will utilize a model with separate, encrypted storage of confidential data. The surface storage and backups will be encrypted using Microsoft's SQL 2008 or 2016 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.

All confidential data will be stored in a Secure Data SQL file. It will be encrypted and stored as binary data type. User IDs are stored separately for those who encrypt and those who decrypt. Only those employees identified as 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 confidential data model used at FTF.

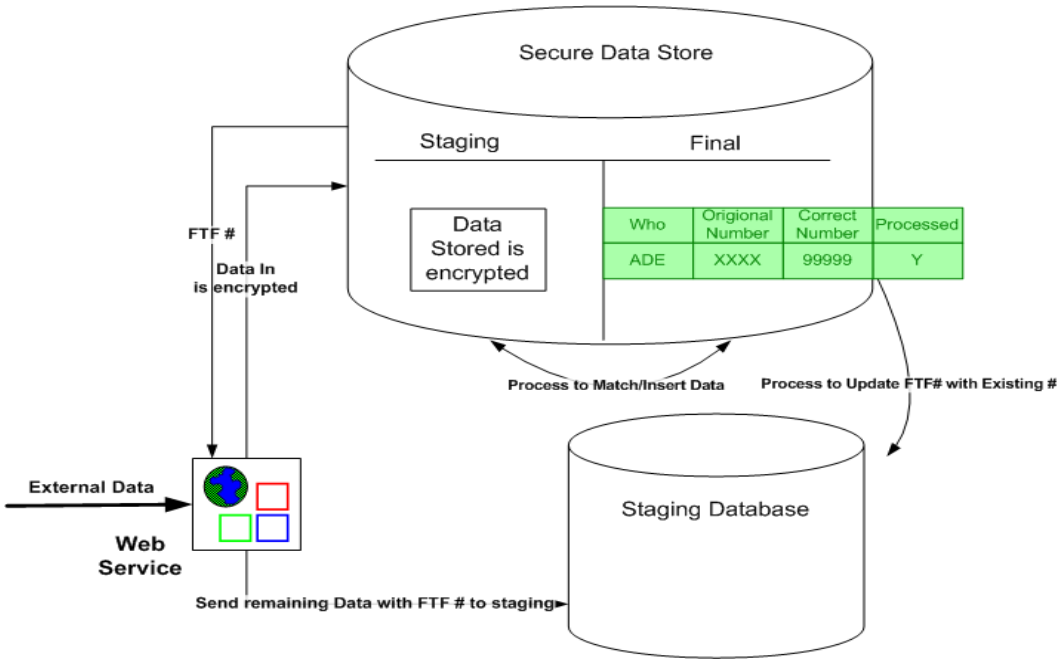
Figure 2: Architecture of Secure Data Store



Confidential data enters 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.

Figure 3 provides an overview of FTF's secure data storage and encryption process.

Figure 3: Secure Data Storage and Encryption Process

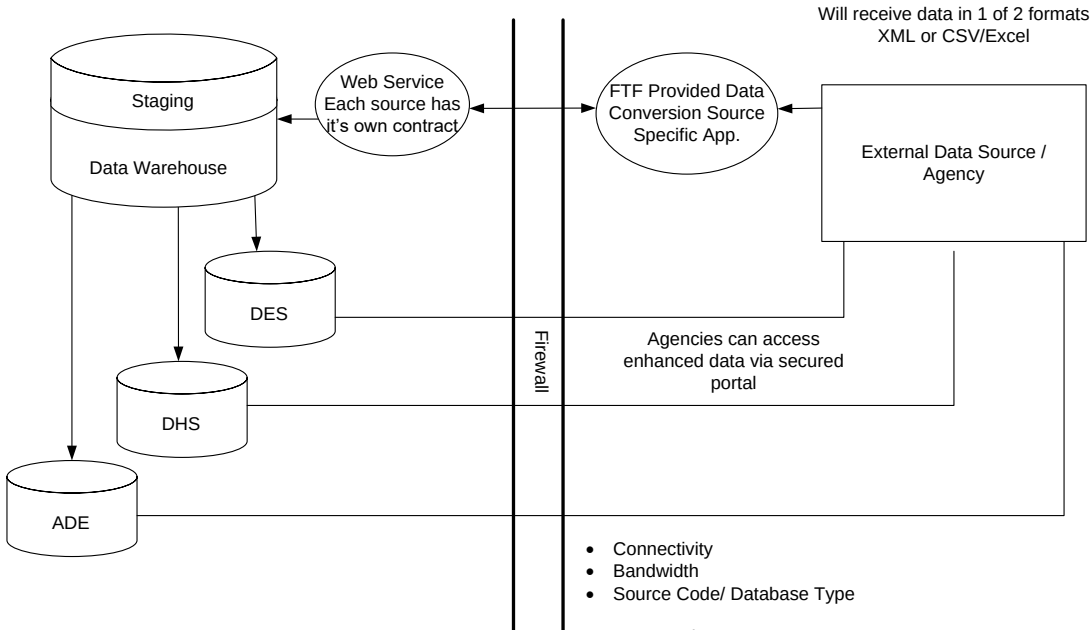


NETWORK ACCESS AND FIREWALL PROTECTION:

FTF'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 is routed through secure firewalls. FTF's firewall technology has 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 are routed through secure gateways and protected by encryption. Secure Socket Layer (SSL) is employed between a web server and browser to authenticate the web server and the user's browser. FTF 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, and key network components will 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:

FTF 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 may be changed periodically by the Operations Division.
- Where badge-reading systems are employed to log access into and out of a secure facility, "piggybacking" of badge holders is prohibited.
- Unused keys, entry devices, etc., are secured.
- Physical access to "critical" IT hardware, wiring, and network devices is controlled for access on a restricted/least privilege basis for the authorized employee or contractor to complete assigned tasks.
- Physical access security measures employed for back-up systems/servers are equivalent to those of the primary system.
- Information systems, media storage areas, and related communication wiring and network devices are 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 data, 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 containing confidential data (disk, tapes, CDs, etc.) are consistently controlled and labeled to guard against misplacement and loss or unauthorized use of information.

BREACH:
An important aspect of FTF data security policies is the effective and timely reporting of all suspected incidents of misuse or loss of confidential data or breaches of data security. FTF will promptly identify, 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) must be notified within 1 hour of the breach.
5. The IT Director will work with the CEO, COO, and Chief Policy Advisor to come up with a communication plan regarding the breach, 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.

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 – State Access Agreement.

EXCEPTIONS:
The Chief Executive Officer (CEO) may approve exceptions to this policy.

Attachments:

A. State Access Agreement

State of Arizona

Access Agreement

I have been made aware and understand that applicable State of Arizona statutes*, rules, policies and directives bind all State of Arizona (State) employees, contractors, vendors, volunteers and other users who have access to the State's technology systems and applications.

[State of Arizona employees] This agreement does not create a contract for employment between any employee and the State. Nothing in this agreement changes the fact that all uncovered employees of the State are at-will employees and serve at the pleasure of the appointing authority.

[Non-State employees/other users (such as, contractors, leased employees, vendors, volunteers, etc.] Nothing in this agreement creates an employment relationship with the State of Arizona.

In consideration for access to State information technology systems and applications, I agree to at all times abide by all applicable Arizona State statutes, rules, policies and directives, and understand that I am prohibited from violating the foregoing, which includes, but is not limited to, the following actions:

1. Revealing data to any person or persons outside or within the agency who have not been specifically authorized to receive such data.
2. Attempting or achieving access to data not germane to my mandated job duties.
3. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts without appropriate authorization.
4. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts for direct or indirect personal gain or advantage.
5. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts maliciously or in retribution for real or imagined abuse or for personal amusement.
6. Unauthorized access, modification or destruction of any computer, computer system, State information system, hardware appliance, network device, media device, computer program, data structure, database, or program code or script.
7. Unauthorized installation or connection of any computer or electronic equipment to a State network.
8. Recklessly disrupting or causing disruption of any computer, computer system or State information system.
9. Unauthorized use of electronic messaging or other communications.
10. Using State equipment or property, including equipment or property leased to the State, for other than work related purposes, unless authorized by written agency policy or other proper authorization.
11. Using a personal device that is not protected with approved and up-to-date anti-virus software and fully patched to access any State of Arizona network.

12. Removing sensitive data from the State network or State devices that are not fully protected with encryption.
13. Using another person's personal data access control identifier (USERID) and password.
14. Revealing my personal data access control identifier and/or password to another person.
15. Asking another user to reveal his/her personal data access control identifier and/or password.
16. Accessing, copying, disclosing, or deleting personally identifiable information, personal health information or other sensitive non-public information beyond that authorized by statute or specific authority of authorizing agent.
17. Accessing, copying, or disclosing critical information technology infrastructure information without authorization.
18. Using software on the local area network (LAN), or on any PC in any manner other than in accordance with the license agreement.
19. Making, acquiring, using, or distributing unauthorized copies of computer software.
20. Bringing in software (from outside the Agency) for use on the LAN or PC without the prior written permission of my Supervisor, Agency Authorizing Authority/Designee and unit responsible for Information Technology.

[State of Arizona employees] All new State employees must be provided with a copy of A.R.S. § 38-448 at the time of authorizing an employee to use an agency computer; the full text of this statute appears below:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

A. Except to the extent required in conjunction with a bona fide, agency approved research project or other agency approved undertaking, an employee of an agency shall not knowingly use agency owned or agency leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sexual acts as defined in section 13-3501. Agency heads shall give, in writing, any agency approvals. Agency approvals are available for public inspection pursuant to section 39-121.

B. An employee who violates this section may be subject to discipline or dismissal.

C. All agencies shall immediately furnish their current employees with copies of this section. All agencies shall furnish all new employees with copies of this section at the time of authorizing an employee to use an agency computer.

D. For the purposes of this section:

1. "Agency" means:

(a) All offices, agencies, departments, boards, councils or commissions of this state.

(b) All state universities.

(c) All community college districts.

(d) All legislative agencies.

(e) All departments or agencies of the state supreme court or the court of appeals.

2. "Information infrastructure" means telecommunications, cable and computer networks and includes the internet, the world wide web, usenet, bulletin board systems, on-line systems and telephone networks.

I agree to seek clarification before entering, modifying, deleting, altering, or disclosing data. I agree to immediately notify my supervisor, manager or any member of the Agency's executive team of any suspected or confirmed unauthorized disclosure or misuse in violation of this agreement or any applicable statutes, rules or policies.

Appropriate action will be taken, including immediate termination of access, to ensure that applicable federal and state statutes, regulations and directives governing confidentiality and security are enforced. Aside from revocation of access, breach of procedures pursuant to this policy or misuse of State property including computer programs, equipment and/or data, may result in prosecution in accordance with any applicable provision of statute, including Arizona Revised Statutes (A.R.S.) Section 13-2316, for computer tampering and/or:

- [State of Arizona employees] I may be subject to discipline or separation.
- [Non-State employees/other users] Violating federal and state statutes and rules, statewide policies, and agency policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring of entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.

During all times that I have access to State information technology systems and applications, I accept responsibility for adhering to all applicable State of Arizona statutes, rules, security policies and directives and agree to abide by this agreement. I understand that I have access to instruction on and access to applicable statutes, rules and policies. Failure to accept the terms of this agreement will mean I will not be permitted access to State of Arizona produced media, data, computer equipment and software.

*Applicable State of Arizona statutes and policies include, but are not limited to:

- A.R.S. § 41-3504. Powers and duties of the department; violation; classification
- A.R.S. § 41-3507. Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure
- A.R.S. § 13-2316. Computer tampering; venue; forfeiture; classification
- A.R.S. § 41-151.12. Records; records management; powers and duties of director; fees; records services fund
- A.R.S. § 41-1750.01. National crime prevention and privacy compact
- [State of Arizona employees] A.R.S. § 38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions
- Statewide Policy 8280: Acceptable Use and corresponding agency policy