Printout Uncontrolled After 10/05/18

TITLE: THIRD-PARTY INFORMATION SECURITY POLICY

PURPOSE: ADTRAN's Information Security Management System is intended to protect ADTRAN's information assets, ensure reliability and integrity of information processing activity, and protect the privacy and legal position of the company and its stakeholders. This document, along with other information security statements, communicate guidelines and your responsibilities that protects ADTRAN's information assets.

APPROVALS:

Title: Vice President, Global Quality
Kent Darzi

FORMS: N/A

REFERENCE DOCUMENTS:
AOP03.02, Information Control Protection
AOP05.09, Information Security Program
AOP05.09.01, ISMS Risk Methodology and Policy
AOP07.06, Supplier Selection Review and Control
ADTRAN Quality Specifications (Q100, 110, 120, 140)

DEFINITIONS: N/A

1.0 RESPONSIBILITY

The ADTRAN Supplier Quality Engineering Department - is responsible to ensure supplier qualification, communicating, and evaluation of suppliers to CP-149 and other ADTRAN Management Systems Policies and Procedures.

ADTRAN suppliers, contractors or other 3rd parties accessing ADTRAN information systems - are responsible to adhere to the information security management system and additional information security policies, guidelines, and procedures administered by ADTRAN's Information Security Managers. Non-compliance to security policies and procedures will be processed in accordance with ADTRAN Management System requirements and the ADTRAN Employee Handbook.

2.0 OBJECTIVE

The objective is to ensure the acceptable use and protection of ADTRAN's information assets and that any misuse of assets is remediated immediately.

3.0 SCOPE

The scope of this policy is any third party which will process any ADTRAN Information. This includes, but is not limited to:

- Third parties involved in the design, development or operation of information systems for ADTRAN e.g. writing and installing bespoke software, third party maintenance or operation of systems, outsourcing of facilities;

- Access to ADTRAN information from remote locations where the computer and network facilities are not under the control of ADTRAN;

- Users who are who are not employees of ADTRAN and require access to ADTRAN information or information systems.

Examples of information assets include (but not limited to):

- Data
  - Office documents
  - Schematics
  - Generated output files
  - Reports
  - etc.
- Information systems equipment, programs and related software applications
  - Business servers
  - Desktops, laptops, and mobile devices
  - Printers, copiers, and fax machines
  - e-mail and text-based system(s)
- Databases, network file storage, cloud file storage, and removable media
- Local, online, and cloud software applications
- Networks and network equipment
- Telephone systems and telephone equipment
  - Telephones
  - Voicemail
- All other computing, data communications and telecommunications environments

4.0 PROCEDURE

4.1 Privacy Statement

1. Users should make no assumption of personal privacy when creating, transmitting or storing personal information on ADTRAN's information systems. All information assets stored or created on ADTRAN's information systems is the property of ADTRAN.
   a. ADTRAN reserves the right to access all information for purposes of ensuring a productive work environment, free of unwanted intrusions and objectionable elements.

2. ADTRAN provides each user a server-based storage location and takes technical and administrative precautions to ensure that other peer users cannot access that location. If required, for purposes mentioned above,
   a. ADTRAN may, to a reasonable degree, instruct qualified IT Department system administrators to retrieve information assets. Users are expected to provide passwords required to open password-protected files.

4.2 Intended Use Guidelines for Corporate Electronic Mail Messaging Systems

1. All messaging, including but not limited to e-mail messages, text messages, attached files, and calendar items, stored in ADTRAN's electronic messaging systems will be purged after 180 days.

2. Users shall not use ADTRAN's e-mail systems to display or communicate confidential or sensitive information to unauthorized recipients.

3. Users shall not use ADTRAN's e-mail systems to display or communicate disruptive, destructive, unproductive, inappropriate or objectionable material.

4. Users are expected to provide passwords required to open password-protected files.

5. Personal use of ADTRAN's e-mail systems is discouraged to the extent that such use would, in management's judgment:

   - Become excessive or create a distraction
   - Limit one's ability to achieve ADTRAN's business goals
   - Introduce information security risks
   - Introduce disruptive, destructive, unproductive, inappropriate or objectionable elements to the work place

6. All information stored in ADTRAN's electronic messaging system is the property of ADTRAN. Users should make no assumption of personal privacy when creating, transmitting or storing personal information on ADTRAN's systems.
   a. ADTRAN reserves the right to access all information for purposes of ensuring a productive work environment, free of unwanted intrusions and objectionable elements.

7. ADTRAN's IT Department provides each user a server-based storage location for electronic messages and takes technical and administrative precautions to ensure that other peer users cannot access that location. If required, for purposes mentioned above,
   a. ADTRAN's IT Department may, to a reasonable degree, instruct qualified IT system administrators to retrieve information stored on this system

4.3 Intended Use Guidelines for Information Systems and Monitoring

1. ADTRAN understands and respect suppliers, contractors', and 3rd parties' individual interests and allows, to a degree, personal activities to be conducted using ADTRAN's information assets. However, the purpose of ADTRAN acquiring these information assets is for the sole purpose of conducting ADTRAN business.

2. In keeping with this goal, systems should be used in a fashion that:

   - Maximizes personal productivity and overall benefit to the company, its customers and its stakeholders
   - Does not subject the company, its customers or its stakeholders to information security risks
   - Does not introduce disruptive, destructive, unproductive, inappropriate or objectionable elements into the workplace

3. Personal use of ADTRAN's information assets is discouraged to the extent that such use would, in management's judgment:
   - Become excessive or create a distraction
   - Limit one's ability to achieve ADTRAN's business goals

- Introduce information security risks
- Introduce disruptive, destructive, unproductive, inappropriate or objectionable elements to the work place

4. All contractors, suppliers, and/or 3rd parties should review the Non-Disclosure Agreement and/or contract for additional security and acceptable use guidelines.

4.4 Security Incident Reporting

1. Contractors, suppliers, and/or 3rd parties are responsible for reporting any misuse or threat to ADTRAN's information assets.

2. All actual or suspected instances of information asset theft, abuse, threat (e.g. hackers, computer viruses, fire, etc.) or obvious control weaknesses affecting (or could affect) security must be reported within 48 hours or sooner to the attention of the ADTRAN IT Information Security Team at 256.963.8502..

5.0 RECORDS

N/A

REVISION HISTORY:

Revision	Author	Date	Change Description
A	Scott McDaniel	10/9/17	NEW
B	Sheryl Dummer	01/26/18	Total reformat and rewrite of policy; Changed approver name and added Third-Party to title.
C	George Giles	10/2/18	Reference Procedures: added AOP7.06 to; Sec. 1: added SQE Department responsibilities.; Removed all references to ADTRAN employees.; Sec. 3: changed scope to address only 3rd parties and not ADTRAN employee; Sec. 4: total rewrite of section to address the management of 3rd parties; 3rd Party ISP: sectionized the policy to make it easier to reference policy requirements; Sec. 2.1: new; Sec. 2.2.new; 3rd Party Policy: added IT Service Desk as contact.

Third-Party Information Security Policy
01/October/2018

1. Background

ADTRAN has a commitment to protect our corporate data and information assets to ensure business continuity and protect against loss from a growing number of security threats. ADTRAN's information security management system was developed to protect ADTRAN's information assets, ensure reliability and integrity of information processing activity, and protecting the privacy and legal position of the company and its stakeholders. ADTRAN uses the ISO 27001 Standard as the foundation for our information security management system and the protection of ADTRAN's information assets.

2. Policy Scope

All 3rd parties accessing ADTRAN information systems are required to adhere to the information security management system and additional information security statement(s) provided by ADTRAN. Non-compliance will be considered unacceptable and could lead to termination of service.

The scope of ADTRAN's information assets includes (but not limited to):

- All ADTRAN data
- All physical locations holding ADTRAN information assets
- All information systems that access, process, or have custody of ADTRAN information assets

Examples of information assets include (but not limited to):

- Data
  - Office documents
  - Schematics
  - Generated output files
  - Reports
  - etc.
- Information systems equipment, programs and related software applications
  - Business servers
  - Desktops, laptops, and mobile devices
  - Printers, copiers, and fax machines
  - E-mail and text-based system(s)
- Databases, network file storage, cloud file storage, and removable media.
- Local, online, and cloud software applications
- Networks and network equipment
- Telephone systems and telephone equipment
  - Telephones
  - Voicemail
- All other computing, data communications and telecommunications environments

2.1. Information Security Reviews

Third parties must document any security elements and controls that have been implemented to comply with this policy in order to assist with any information security audits carried out by the BBC or nominated parties.

2.2. Exceptions

Third-Party Information Security Policy
01/October/2018

Where third parties are unable to meet any of the control requirements defined in this policy then approval will be required from the ADTRAN Information Security Team and/or to ADTRAN Global Quality. Please contact Information.Security@adtran.com first instance

3. Privacy Statement

Users should make no assumption of personal privacy when creating, transmitting or storing personal information on ADTRAN's information systems. All information assets stored or created on ADTRAN's information systems is the property of ADTRAN. ADTRAN reserves the right to access all information for purposes of ensuring a productive work environment, free of unwanted intrusions and objectionable elements.

ADTRAN provides each user a server-based storage location and takes technical and administrative precautions to ensure that other peer users cannot access that location. If required, for purposes mentioned above, ADTRAN may, to a reasonable degree, instruct qualified IT Department system administrators to retrieve information assets. Users are expected to provide passwords required to open password-protected files.

3.1 Intended Use Guidelines for Corporate Electronic Messaging Systems

All messaging, including but not limited to e-mail messages, text messages, attached files, and calendar items, stored in ADTRAN's electronic messaging systems will be purged after 180 days.

Users shall not use ADTRAN's e-mail systems to display or communicate confidential or sensitive information to unauthorized recipients.

Users shall not use ADTRAN's e-mail systems to display or communicate disruptive, destructive, unproductive, inappropriate or objectionable material.

Users are expected to provide passwords required to open password-protected files.

Personal use of ADTRAN's e-mail systems is discouraged to the extent that such use would, in management's judgment:

- Become excessive or create a distraction
- Limit one's ability to achieve ADTRAN's business goals
- Introduce information security risks
- Introduce disruptive, destructive, unproductive, inappropriate or objectionable elements to the work place

All information stored in ADTRAN's electronic messaging system is the property of ADTRAN. Users should make no assumption of personal privacy when creating, transmitting or storing personal information on ADTRAN's systems. ADTRAN reserves the right to access all information for purposes of ensuring a productive work environment, free of unwanted intrusions and objectionable elements.

ADTRAN's IT Department provides each user a server-based storage location for electronic messages and takes technical and administrative precautions to ensure that other peer users cannot access that location. If required, for purposes mentioned above, ADTRAN's IT Department may, to a reasonable degree, instruct qualified IT system administrators to retrieve information stored on this system.

3.2 Intended Use Guidelines for Information Systems and Monitoring

ADTRAN understands and respect Users' individual interests and allows, to a degree, personal activities to be conducted using ADTRAN's information assets. However, the purpose of ADTRAN acquiring these information assets is for the sole purpose of conducting ADTRAN business.

In keeping with this goal, systems should be used in a fashion that:

- Maximizes personal productivity and overall benefit to the company, its customers and its stakeholders
- Does not subject the company, its customers or its stakeholders to information security risks
- Does not introduce disruptive, destructive, unproductive, inappropriate or objectionable elements into the workplace

Personal use of ADTRAN's information assets is discouraged to the extent that such use would, in management's judgment:

- Become excessive or create a distraction
- Limit one's ability to achieve ADTRAN's business goals
- Introduce information security risks
- Introduce disruptive, destructive, unproductive, inappropriate or objectionable elements to the work place

All contractors, suppliers, and/or 3rd parties should review the NDA and/or contract for additional security and acceptable use guidelines.

4. Security Incident Reporting

All actual or suspected instances of information asset theft, abuse, threat (e.g. hackers, computer viruses, fire, etc.) or obvious control weaknesses affecting (or could affect) security must be identified and communicated in a timely manner to the attention of the IT Service Desk (servicedesk@adtran.com), and/or the ADTRAN IT Information Security Team at (+1) 256.963.8502.