1. **Company Information**

Turning Technologies LLC  
255 W Federal Street  
Youngstown, OH 44503  
866-746-3015

**About Turning Technologies**
Turning Technologies is the leading global partner for learning engagement and assessment services focused on measurably improving teaching and learner success. Our solutions manage, enhance and deliver instructional and assessment content in ways that improve learner success while collecting critical data for use in meaningful ways. Founded in 2002, the company began with the development of response technology that was affordable, user-friendly and better documented so that users could easily grasp its benefits. Today, over 20 million response devices have been delivered to K-12 schools, universities, government agencies, military bases and businesses worldwide. In 2013 Turning acquired industry pioneer eInstruction with more than 30 years of experience and a diversified solution to expand both its market share and product offerings across all industry segments. The combined portfolio of clicker systems, polling software, assessment platforms, interactive whiteboards and professional development services are designed to inspire achievement each and every day. Founded and based in Youngstown, OH, Turning maintains global offices in Scottsdale, AZ, Fort Wright, KY, Belfast, United Kingdom and Amsterdam, the Netherlands.

Main Website: [https://www.turningtechnologies.com/](https://www.turningtechnologies.com/)  
Turning Account: [https://account.turningtechnologies.com/account/](https://account.turningtechnologies.com/account/)  
Help Requests: [https://turningtechnologies.zendesk.com/anonymous_requests/new](https://turningtechnologies.zendesk.com/anonymous_requests/new)

Turning Technologies LLC is owned 100% by Turning Tech Holdings, LLC. Turning Tech Holdings, LLC is owned 100% by our parent company, Turning Tech LLC.

**Executive Officers**
Mike Broderick, CEO  
Dave Kauer, COO  
Dr. Tina Rooks, CIO

**1.1 Key Personnel/Support Descriptions**

**Dr. Tina Rooks**  
SVP & Chief Instructional Officer  
[trooks@turningtechnologies.com](mailto:trooks@turningtechnologies.com)
Security Document Template

Fares Bouchedia
VP of Software R&D
fbouchedia@turningtechnologies.com

John Sofko
Director of Cloud Operations
jsofko@turningtechnologies.com

- Creating, distributing and maintaining a formal Incident Response Plan.
- Ensuring all appropriate personnel are aware of and comply with this and all other Turning Technologies policies.
- Creating appropriate performance standards, control practices and procedures designed to provide reasonable assurance that all employees observe this policy.
- Request various changes to an employee’s security profile in writing via the Security Profile Request Form and provide justification for the change.
- Provide employees with the security policy and obtain a signed receipt from the employee.

Manager of Information Technology
The Manager of Information Technology is ultimately responsible for all IT design, configuration implementation and maintenance of IT infrastructure for the company.

The Manager of Information Technology is responsible for:
- Developing and maintaining written standards and procedures necessary to ensure implementation and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

Network Administration Team
The Network Administration Team is responsible for implementing, maintaining and monitoring the IT infrastructure. This team will report to the Manager of Information Technology.

The Network Administration Team’s duties will consist of:
- Creating, modifying or deleting users with approval by the Manager of Information Technology.
- Maintaining a list of administrative passwords in secure physical and electronic areas.
- Ensuring need to know access is granted to each user account based on job function.
- Ensuring that only approved local user accounts exist.
- Ensuring all approved auditing and monitoring functions are implemented.
2. Product/Software Descriptions

TurningPoint Cloud Description

- Turning Technologies recommends industry-leading TurningPoint Cloud for PC and Mac. TurningPoint Cloud is the industry’s most robust software offering a native integration with PowerPoint®, on-the-fly polling over top of any application, as well as integrated self-paced mode for tests, quizzes and course evaluations. TurningPoint Cloud can be used with traditional clickers and web-enabled mobile devices via ResponseWare.
- TurningPoint Cloud is an interactive polling software tied to a cloud-based interface. The software leverages the same familiar desktop application as previous TurningPoint versions with added enhancements.
- TurningCloud accounts are available for both instructors and students to leverage a secure, cloud-based management of courses, rosters and assessment data. Secure login and file encryption ensures data is safeguarded to protect both the university and its student population while providing one, central location for data management and assessment.

2.1 Customer Support

Routine concerns can be logged with Customer Support by phone, email or through our help ticketing system. Emergency requests can be reported to Customer Support for immediate escalation. Phones are answered on weekdays between 8:00am and 9:00pm EST. Additionally, emergency requests can be sent directly to:

Fares Boucheddid, VP of Software R&D, fbouchedid@turningtechnologies.com
John Sofko, Director of Cloud Services, jsofko@turningtechnologies.com

Turning Technologies offers Single Sign On support to integrate with the university’s centrally managed authentication service. However, user credentials will not be stored on the Turning Technologies servers.


3.1 General Overview

The following points constitute the underlying tenets that dictate or clarify all security policies put in place. They should be the basis upon which all rules are built.

- Turning Technologies run private and public networks.
  - Internet users should be able to access our public resources in the most speedy, efficient manner, while protecting the integrity and security of the content.
  - Internet users should not be able to access our private resources directly.
Security Document Template

- Turning Technologies performs criminal background checks and reference checks on all employees and contractors.
- Turning Technologies has customers and business partners who need additional access permissions to network resources.
  - These users should be evaluated on an individual basis and only granted minimum access needed to accomplish the particular requirement.
  - In no case should these users be granted access that would allow them to access content that they do not own.
  - In no case should these users be granted access that would allow them to place unapproved executable code on a shared production server.
  - Access by customers and business partners should be logged.
  - In the event a partner or contractor is working on or has access to Turning Technologies source code or software, an NDA will be signed and countersigned by all parties.
- Turning Technologies employs contract employees as needed. Contract employees must follow all employee responsibilities described in the corporate Information Security Policy and the Data Security Policy.
- Turning Technologies employs a producer-publisher model for placing content on production servers.
  - The ability to write content to production servers should be limited to approved employee publishers.
  - The ability to produce content destined for public production servers should be limited to approved employee producers and approved non-employed partners.
  - Publishing of content should be logged.
- All Turning Technologies employees need varying access to resources on the network to accomplish their jobs, but management recognizes that statistically, employee precipitated security breaches far outnumber other types of security breaches.
  - Employees’ job descriptions and technical abilities should be evaluated on an individual basis. Employees should be granted access to all resources needed to accomplish daily job duties, without jeopardizing production content in any way. Of course, the producer-publisher model and the principal of least privilege must also be enforced.
  - Remote access to Turning Technologies’ VPN should be granted only to employees who demonstrate a specific business need.
  - All employee access is logged and stored for 6 months.
  - Internal resources are limited so that only approved employees can access the resources both internally and remotely.
- Electronic security is easily bypassed if sufficient physical security is not enforced.
  - Only authorized employees have physical access to the building.
  - Workstations should not be useable when the employee is not physically present.
Physical access to the NOC should be limited to approved employees, and only during the times and days required to accomplish their duties. All physical access should be logged and monitored. Visitors must sign in and out of the facility, and the visitor log must be maintained at least 6 months. All visitors must be accompanied by an employee at all times.

Security Training for Employees: Employees are educated on Information Security and Acceptable Use during new hire training. The Acceptable Use Policy must be signed by the employee before (s)he is granted access to company resources. Current employees are reminded to review Information Security and Acceptable Use on an annual basis. The Security Officer will be responsible for ensuring that these rules are followed.

- Turning Technologies performs criminal background checks and reference checks on all employees and contractors.
- All employees sign Turning Technologies’ NDA at the point of employment which is ongoing for the duration of their employment.
- Termination or transfer of employees is handled by our HR department and includes retaining all user equipment and officially transferring appropriate access over to immediate supervisor.

3.2 Building Security

- Turning Technologies provides 24/7 building access to full time employees for business purposes only. This is controlled and monitored through the use of keycards. Employees are to carry the assigned keycard at all times.
- Employees are not allowed to share or exchange keycards with other employees.
- Employees are responsible for the keycard that (s)he has been assigned. If the card has been lost or stolen then the employee must contact the IT Manager or HR Manager immediately so it can be deactivated. If the card is not recovered then a replacement card will be reissued for a $5 fee to the employee.
- Employees are not to bring unattended guests into the building.
- Employees are not to allow non-employees into the building without contacting or escorting the person that (s)he is here to see.

3.3 Credit Card Security

Since we are not PCI compliant, we offload our credit card processing to a PCI compliant third party, 3Delta Systems: [http://www.3dsi.com](http://www.3dsi.com).

3Delta Systems is a highly secure system designed to comply with:
- PCI DSS: Payment Card Industry Data Security Standard
- FFIEC: Federal Financial Institutions Examination Council
- HIPAA: Health Insurance Portability and Accountability Act
- SarbOx: Sarbenes-Oxley Accounting Compliance Requirements
3.4 Other Security

How to identify new laws with security implications: We have not completed SAS-70 or ISO 27001. Our hosting provider (AWS) provides their SAS-70 report here: http://aws.amazon.com/compliance/soc-faqs/

4. Network Description

Turning Technologies recognizes that network security is a key aspect of overall data security. It is therefore the responsibility of the IT Department to build and maintain a safe and secure network environment.

4.1 Network Layout:

Turning Technologies will operate a segmented network. The purpose of this network segmentation is to provide a high level of security. Access across segments will be controlled through firewall rules or Access Control Lists. This will allow only authorized traffic between segments.

Defined Network Segments

- Production Servers
- Test Servers
- Development Servers
- Corporate Access
- Guest Access

4.2 Corporate Wi-Fi

Turning Technologies has implemented a corporate Wi-Fi network. This net is to be used by employees while working in different areas of the building. The Network Administration Team is responsible for configuring and maintaining this network.

The following rules must be followed regarding Wi-Fi networks:

- All Wi-Fi networks are to be configured using WPA2.
- All Wi-Fi networks are to be encrypted using AES.
- Only authorized equipment is to be connected to the Corporate Wi-Fi network.
- Guest access is allowed however, the following rules must be followed:
  - The guest Wi-Fi network is segmented from the corporate Wi-Fi network.
  - The guest Wi-Fi network is bandwidth restricted.
  - The guest Wi-Fi network is given lower priority over corporate traffic.
Security Document Template

4.3 Corporate VPN

Turning Technologies provides a VPN to facilitate secure, authenticated access to the company electronic resources from remote locations. Improper use of the employee VPN can pose a significant security risk to the company. The Network Administration Team is responsible for configuring and maintaining the VPN.

The following rules must be followed regarding the VPN:
- The VPN shall be encrypted using AES.
- Only authorized computers shall be connected to the VPN.
- Only employees, approved contractors, subcontractors and vendors are allowed to connect to the VPN.
  - Approval of non-employees must be granted by the Manager of Information Technology and the Security Officer.
  - Accounts are to be created with a need to know access.

4.4 Firewall Configuration

Turning Technologies will incorporate the use of network firewalls at the edges of the network as well as in between segments. The following rules must be followed regarding access, configuration changes and maintenance to all network firewalls.

- Configuration changes will be followed based on the Change Control Policy.
- Access to firewall configuration is restricted to the Network Team and any subcontractor approved by that team.
- A list of ports and services necessary for business purposes will be documented in Network Management section of the Master IT Policy and Best Practices document.
- All unused ports above 1024 will be blocked (Incoming and Outgoing).
- Support and maintenance contracts are the responsibility of the IT Manager.
- Software and firmware updates to the firewall are to follow the Patch Management guidelines found within this document.
- Firewall configurations will be backed up and stored in a secure location. This location will be documented in the Configurations section of the Master IT Policy and Best Practices document.
- Port Address Translation and Network Address Translation will be used to prevent internal systems from directly being accessed via the Internet.
- Firewall rules are to be reviewed and compared to the documented rules on a quarterly basis. Any discrepancies are to be investigated and documented by the Security Officer.
4.5 Network Monitoring

To ensure that Turning Technologies’ network is safe and secure the IT Department is responsible for analyzing system, application and network logs. Specifics on monitoring and log collection will be documented in the Master IT Policy and Best Practices. The following rules apply.

- Audit logs for all system components will include:
  - Login successes/failures
  - File access successes/failures
- Logs should be sent to a central logging server.
- Notifications should be setup for possible attacks or access violations.
- Logs should be reviewed daily.
- Logs are to be backed up daily.
- Logs are to be kept as historical data for one (1) year.

4.6 Network Access

Turning Technologies makes every effort in order to keep safe and secure networks and office facilities. The implementation of access controls for data and facility access are used to accomplish this. It is the responsibility of the IT Department to create and maintain the access controls that are used to maintain this security. It is the responsibility of the HR Manager to notify the IT Department when a new employee is hired or an existing employee is terminated. It is also the responsibility of the HR Manager to notify the Manager of Information Technology or the Security Officer if an employee has been deemed a potential security risk.

All access to data and company resources must be controlled by unique usernames and passwords. The following account control rules must be followed regarding the creation of user accounts.

- All accounts require a secure password and must follow the company’s Password Policy.
- All accounts are created with a need to know basis.
- All account creation or modifications must be logged in the company’s Change Control System.
- All accounts will be automatically locked for 30 minutes after 5 failed login attempts.
- Systems with inactive logins will automatically lock or logoff after no more than 15 minutes of inactivity.
- Accounts for testing will be disabled immediately following the test completion.
- Unused accounts are to be disabled.
- Physical access to hard copy versions of confidential or sensitive data that is created or given to Turning Technologies is treated with need to know access.
- Active hard copy data is stored securely when not in use and is not left unattended.
Security Document Template

- This information must be labeled as confidential or sensitive on every page.
- Each page is to have a creation date.
- Each page is to have a validity date.
- Hard copies are to be destroyed by an approved shredding device at the end of its lifecycle.

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee’s job duties. Access control requirements are defined within the Data Security Policy.

Physical access to Turning Technologies facilities will be secured with either RFID access cards or a physical key. This is to provide security for all personnel, equipment and data for the company. The following building access rules apply and are stated in the companies Acceptable Use Policy.

- Turning Technologies provides 24/7 building access to full time employees for business purposes only.
- Each employee will receive a RFID access card and if necessary a physical key.
- Employees are required to carry their access cards at all time and must not share or exchange access cards with other employees.
- Employees are not to bring unattended guests into the building.
- Employees are not to allow non employees into the building without contacting or escorting the person that (s)he is here to see.

4.7 Identity Management

Turning Technologies utilizes user accounts in order to manage access to data and systems within the network. It is important for these accounts to remain secure in order to reduce the risk of an account being compromised. Therefore, it is the duty of every employee to follow the requirements that are detailed in the Password Policy.

4.8 Anti-Virus Software

The use of Anti-Virus Systems is critical in securing the company network. Therefore the IT Manager and Security Officer will be responsible for the implementation and management of all Anti-Virus systems. The following rules must be followed regarding access, configuration changes and maintenance to all Anti-Virus Systems.

- Configuration changes will be followed based on the Change Control Policy.
- Access to Anti-Virus System configuration is restricted to the Network.
- All signatures must be updated at least once a day.
- All systems must be updated at least once a year.
- Approved Anti-Virus systems are to be documented in the Network Management section of the Master IT Policy and Best Practices document.
Security Document Template

- Computers, network traffic and email are to be scanned.
- Anti-Virus logs are to be reviewed daily.

4.9 Segmented Network

Turning Technologies will operate a segmented network. The purpose of this network segmentation is to provide a high level of security. Access across segments will be controlled through firewall rules or Access Control Lists. This will allow only authorized traffic between segments.

4.10 Patch Management

IT Staff is responsible for the overall patch management implementation, operations and procedures. While safeguarding the network is every user's job, IT Staff ensures all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. IT Staff will assess the effect of a patch to the corporate infrastructure prior to its deployment. The department will also assess the affected patch criticality relevant to each platform (e.g., servers, desktops, printers, etc.).

5. External Parties/Hosting

Information will be stored at locations outside of the physical control of the university. Turning Technologies uses Amazon Web Hosting for all hosting and specifically the AWS us-east-1 (N. Virginia).


Amazon Web Services for hosting and occasionally third parties development firms with specified expertise. NDAs are signed by all third parties and stored digitally on our internal knowledge platform. In addition to NDAs, VPN controls are also in place.


Turning Technologies uses AWS and adhere to their recovery processes that are not customer facing.

Security Administration is performed using AWS Identity and Access Management (AWS IAM), key management and rotation, temporary security credentials and multi-factor authentication (MFA). AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.
Security Document Template

AWS has implemented security management processes, PCI controls and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements.

Individual AWS services and hosted servers are secured using AWS Identity and Access Management (IAM). IAM provides a role-based system for controlling access to services and servers. The TurningPoint Cloud architecture utilizes IAM roles to limit the group of administrators that are authorized to sign in to the hosted services and servers. IAM roles are also utilized to control the actions that each type of hosted server is allowed to perform within the AWS service environment.

TurningPoint Cloud utilizes AWS firewalls and security groups to limit communication between service layers and between individual servers. TurningPoint Cloud is hosted by our own Virtual Private Cloud (VPC) within the AWS infrastructure. This VPC architecture provides additional isolation for the TurningPoint Cloud application.

AWS takes many steps to ensure the physical security of their data centers. The first of these measures involves "limiting knowledge of the location of the data centers to those within Amazon who have a legitimate business reason for this information." For employees that are authorized to access the data center, "physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Within each region, AWS offers multiple availability zones. Each availability zone is an isolated infrastructure segment that is connected via a low-latency link to the other availability zones in the region. In the event of an infrastructure failure, it is unlikely that the failure would affect multiple availability zones. TurningPoint Cloud is designed to utilize services in many different availability zones to minimize application service disruption. AWS servers are under 24 hour monitoring and system monitoring alerts are in place in order for immediate response to identified issues.

In the case that Turning Technologies becomes aware that a data breach has occurred on AWS, we will leverage email notifications as well as account dashboards to alert our customers within 24 hours of our first knowledge of this event. We will include all
necessary instructions to our customers and continue to provide updated information until we believe the situation has been remedied.

A list of permissions or rules exists for accessing an object or network resource. In Amazon EC2, security groups act as ACLs at the instance level, controlling which users have permission to access specific instances. In Amazon S3, you can use ACLs to give read or write access on buckets or objects to groups of users. In Amazon VPC, ACLs act like network firewalls and control access at the subnet level.

The firewall requires Turning Technologies X.509 certificate and key to authorize changes, thus adding an extra layer of security. AWS supports the ability to grant granular access to different administrative functions on the instances and the firewall, therefore enabling additional security through separation of duties.

6. General Security

6.1 Encryption

All data is encrypted using AES 128. AES 128 Encryption is used for data at rest and data in transfer. TurningPoint Cloud will deploy enterprise-grade encryption for all participant and session files, while maintaining an intuitive user experience. Industry standard AES-128 encryption ensures that if a non-authenticated user obtains a file from our solution, data will not be accessible. Encryption of files as faculty port data between classroom and office is critical to ensure access control, while maintaining a typical faculty user workflow.

TurningPoint Cloud encrypted participant and session files will not be backwards compatible with previous versions of TurningPoint due to the added layer of AES encryption (unavailable in previous releases). Additionally, encrypted files will require the file owner to login in order to view data. Sharing of files will be tightened in order to adequately support security enhancements and ensure protection of student data.

The protection of customer data is a very important requirement of the TurningPoint Cloud system. TurningPoint Cloud contains Personal Identifying Information (PII) in the form of first and last name, email address and (potentially) student identification number. In order to secure this PII data at rest, these fields are encrypted within the AWS Relational Data Store (RDS) database using industry “best practice” encryption technologies.

6.2 Risk/Vulnerability Assessment and Remediation

Turning Technologies makes every effort to ensure that no data is lost or services are disrupted. However, in the event of such an incident the company will follow the approved Disaster Recovery and Business Continuity Plan. It is the responsibility of the
Security Document Template

Manager of Information Technology to develop and maintain this plan. The Manager of Information Technology will also be responsible for the plans execution.

To ensure that the network, applications and servers are secured properly, the IT Department will be tasked with system and penetration testing. These tests should be performed on an annual basis and the results documented. All testing procedures will be documented in the Master IT Policy and Best Practices document.

Testing should include but not limited to:
- Account/Group Access
- Port Scanning
- SQL Injection
- Vulnerability Scanning

6.3 Mitigating Security Incidents

Turning Technologies complies with all laws regarding intellectual property. Turning Technologies and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose Turning Technologies and the responsible employee(s) to civil and/or criminal penalties. This applies to all software that is owned by Turning Technologies, licensed to Turning Technologies, or developed using Turning Technologies resources by employees or vendors. The Manager of Information Technology is responsible for ensuring that the company is compliant with all software licenses. Employees are to follow the rules laid out in the General Computer Use section of the Acceptable Use Policy regarding the installation of software.

6.4 Software Development Security

Turning Technologies develops solutions for the audience response market. It is the goal of the company to develop the most secure, reliable and easy to use solutions for our customers. The Director of Hardware Development and the Director of Software Development are responsible for making sure that the technologies that the company offers meet these goals.

Industry best practices must be followed for all products developed throughout the product lifecycle including:
- Data protection requirements are to be gathered during the requirements phase of product development.
- Review company security polices and requirements annually.
- Testing patches and firmware before deployment.
- Testing configuration changes before deployment.
- Separate environments for development, testing and production should exist.
- Production data is not to be used for testing or development.
Security Document Template

- All test data must be removed prior to deployment.
- All usernames and passwords must be removed prior to deployment.
- Custom code must be reviewed prior to deployment.
- Back-out procedures must be in place prior to deployment.
- Only approved staff members may release products into the production environment.
- The use of strong encryption is to be used when transmitting, receiving or storing sensitive or confidential information.

We ensure that our software is coded correctly to properly handle multiple tenants and follow best practice coding standards as well as QA standards to ensure data remains separated by tenant. Controls we implement provide assurance that data integrity is maintained through all phases including transmission, storage and processing.

6.5 Hardware Based Firewall

The firewall requires Turning Technologies X.509 certificate and key to authorize changes, thus adding an extra layer of security. AWS supports the ability to grant granular access to different administrative functions on the instances and the firewall, therefore enabling additional security through separation of duties.

7. Disaster Recovery Plan

Turning Technologies makes every effort to ensure that no data is lost. However, the company recognizes that data corruption and loss may happen sometime. It is the responsibility of the IT Department to implement, configure and maintain all data backup systems for the company. These processes are documented within the Disaster Recovery Plan.

The following rules must be followed regarding backup processes:
- Backups are taken frequently based on the nature of the data.
- Backups are only accessed by the IT Department.
- All backup jobs are monitored.
- Backups are kept offsite.
- Backups are kept for at least 30 days.

8. Media/Hardware Handling and Disposal

All digital media that may contain sensitive data must be destroyed when it is no longer needed.
Digital media may include but is not limited to the following:

- CDs
- DVDs
- Flash Drives, Thumb Drives, USB Drives
- Memory Cards
- Floppy Disks

All hardware that may contain sensitive data must be processed by the IT Department before it is transferred to another employee, exchanged for warranty replacement or decommissioned. This is to ensure that the integrity of the data is not compromised.

Regarding disposal, the IT Department will follow these rules:

- Hardware transfers within the company must go through a simple formatting process.
- Hardware sales must be formatted no less than 3 times.
- Failed/failing non warranty hardware is physically destroyed before disposal.
- Failed/failing warranty hardware should be formatted no less than 3 times if possible before it is exchanged with the manufacture.
- Printers/copiers hard drives are to be formatted no less than 3 times or destroyed before disposal.

9. Change Management

Having a Change Control policy is critical to Turning Technologies ability to maintain stable and secure networks and products. The Director of Hardware Development, the Director of Software Development and the IT Manager will be responsible for ensuring that the Change Control Policy is implemented and followed in their respective environments.

The following rules must be followed regarding changes made to network infrastructure, telecommunication infrastructure and product development:

- A formal change request must be submitted for all changes. Change approval must be appropriate to the magnitude, risks and criticality of the change.
- All requests must be reviewed to determine any potential failures/negative impact.
- All changes must be approved by department heads before the change is made.
- A log for all changes are kept with the following information:
  - Change Requestor
  - Change Request Date
  - Change Requested
  - Change Approver
  - Change Approved Date
  - Change Implementer
  - Change Implementation Date
Security Document Template

- All changes must be tested and validated.

10. Change Management

All references have been customers for multiple years.

Jon Dorbolo
Oregon State University
jon.dorbolo@oregonstate.edu

Lesley Speller
University of Arkansas
lspelle@uark.edu

Suzanne Hess
Drake University
suzanne.hess@drake.edu

11. Available Documentation

- ISOS 27002 Certificate
- AWS Disaster Recovery Document
- AWS Security Whitepaper
- TT FERPA Compliance Review
- TT Security Whitepaper
- FERPA Compliance Verification