OFFICIAL NOTICE AND AGENDA OF A MEETING OF THE BOARD OF DIRECTORS OF THE CITY-COUNTY INFORMATION TECHNOLOGY COMMISSION

Meeting: City County Information Technology Commission Board Meeting
Members: Lance Leonhard (C), Maryanne Groat, Gary Olsen (S), Doug Diny, Kurt Gibbs (V), Chet Strebe, Jason Hake
Location: Board Room - 2nd Floor - City Hall
Date/Time: November 5, 2024 7:30 a.m.

AGENDA ITEMS FOR CONSIDERATION

1) **Call Meeting to Order**
2) **Public Comment** (Not to Exceed 15 Minutes)
3) **Approval of the Minutes of the October 1, 2024 CCITC Board Meeting**
4) **Educational Presentations and Board Discussion**
   a) TDX Dashboard Data Review
   b) Project Updates
   c) Workplan Update
5) **Operational Functions required by Statute, Ordinance, Resolution or Existing CCITC Policy:**
   a) Discussion and possible action approving the Security Program Policy
   b) Discussion of the schedule for the Director's Performance Review
6) **Announcements**
   a) Next meeting is December 3, 2024 at 7:30 am in the City Hall Board Room and via WebEx.
7) **Adjournment**

SIGNED: *Gerard M Klein*
GERARD M. KLEIN, DIRECTOR

Persons wishing to attend the meeting by phone may call into the telephone conference beginning five (5) minutes prior to the start time indicated above using the following number: 1-408-418-9388. Access Code: 962 376 748. If you are prompted to provide an "Attendee Identification Number," enter the "#" sign. No other number is required to participate in the telephone conference.
When you enter the telephone conference, PLEASE PUT YOUR PHONE ON MUTE!

This agenda was faxed to the Wausau Daily Herald, and City Pages on 11/01/2024 at 8:45am. by Carol Langbehn

This notice was posted on the Marathon County & City of Wausau websites on 11/01/2024.

Please note that, upon reasonable notice, efforts will be made to accommodate the needs of disabled individuals through appropriate aids and services. For additional information or to request this service, contact Gerard M. Klein, Director CCIT, at 407 Grant Street, Wausau. WI 54403-4737 or telephone (715) 261-6700.

CITY-COUNTY INFORMATION TECHNOLOGY COMMISSION (CCIT)

Date: October 1, 2024, 7:30 a.m. City Hall Board Room

Members present: Lance Leonhard (C), Gary Olsen, Kurt Gibbs, Doug Diny, Maryanne Groat, Jason Hake, Chet Strebe

Members Absent:

Additional Attendees: Gerard Klein, Wesly Yuds, Tami Coulson, Dale Schirmacher, Steve Wettern

1) **Call Meeting to Order:** The meeting was called to order by Lance Leonhard at 7:33 a.m.
2) **Public Comment:** There was no public comment.
3) **Approval of the Minutes of September 10, 2024 CCITC Board Meeting: Olsen/Strebe** moved/seconded to approve the minutes of the September 10th meeting. **Carried.**
4) **Educational Presentations and Board Discussion**
   a) TDX Dashboard Data Review: The Board received a report and Wesly Yuds reported that there is nothing unusual about the data presented in the report.
   b) Project Updates
      - Adaptive Budgeting is wrapping up
      - Gravity implementation is in the training phases.
      - Single sign on: Looking at how to move forward, also considering changing password requirements.
      - Rapid 7 implementations have gone well. It has given us the ability to correlate multiple events to improve detection of security concerns.
      - Medical Examiner software contract has been signed.
   c) Budget vs Actual Report: The Board reviewed the report with no questions.
   d) Information Security Program Policy: Dale Schirmacher reviewed the Information Security Program Plan with the Board. He requested that the Board review the document, and it be up for approval at the next Board meeting.
5) **Operational Functions required by Statute, Ordinance, Resolution or Existing CCITC Policy:**
   a) Discussion and possible action to add additional support for Riverside Fire District (Add PC support to our existing support for their mobile devices): Director Klein informed the Board of the current service provided. CCITC provided Riverside Fire a proposal to extend services to their office computer equipment. Director Klein asked the Board if there are any concerns about extending the additional support. Chairman Leonhard expressed concern as to whether it would impact partner services. He deferred to Director Klein. The Board discussed concerns on moving forward with the potential merger of SAFER and Riverside Fire Department. **Olsen/Strebe** moved/seconded to authorize Director Klein to enter a contract with a 90 day out clause if CCITC moves forward to provide services. **Carried.**

b) Discussion and possible action to Approve 2025 Budget: Director Klein reviewed the potential cost savings that were considered. Director Klein reviewed the changes to the budget since the last Board meeting. Olsen suggested looking at ways to reduce software costs by looking for opportunities for cost savings. The Board requested an evaluation of costs to identify potential cost savings for 2026. **Olsen/Groat** moved/seconded to approve the budget as presented. **Carried.**

c) Discussion and possible action approving changes to Intergovernmental Agreement and its associated Operating Agreement: Director Klein reviewed the documents and made updates to simplify and reflect current practice. These documents would need to be approved by the governing boards of each of the partner organizations. **Gibbs/Olsen** moved/seconded to approve the Intergovernmental Agreement and Operating Agreements and have them approved by the governing boards. **Carried.**

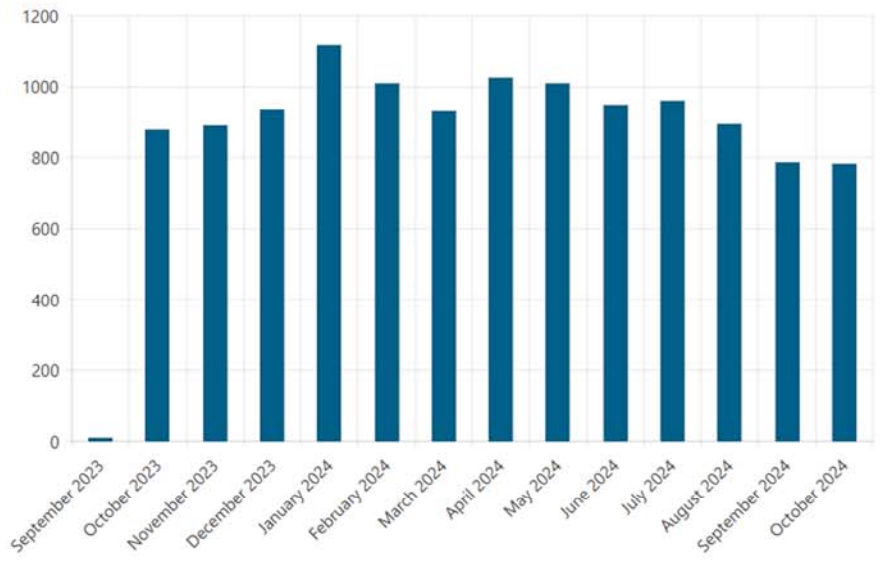
d) Discussion and timeline regarding process to be employed for the Director's annual review. Chairman Leonhard informed the Board that he will be sending the review for to the Board members today and requested that the documents be returned to him by the end of October.

6) Announcements

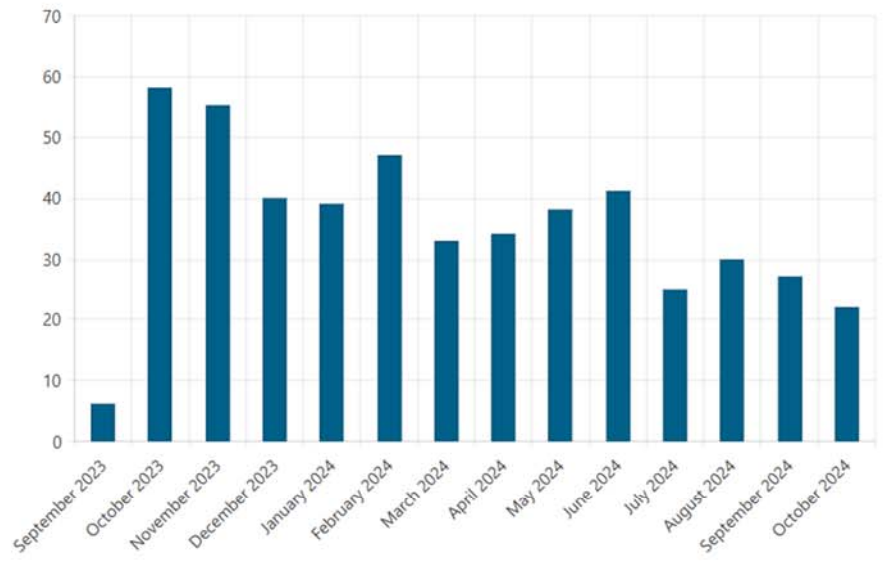
a) Next meeting is November 5, 2024 at 7:30 am in the City Hall Board Room and via WebEx.

7) Adjournment Motion by Diny/Olsen Motion carried. 8:38AM

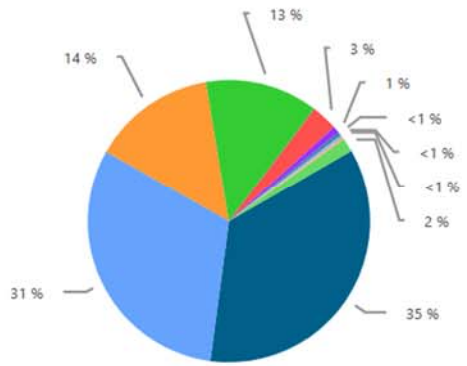
Tickets Year to Date



On Call Tickets Year to Date

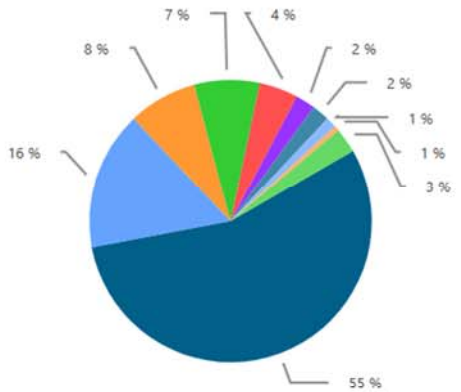


Tickets by Entity Year to Date



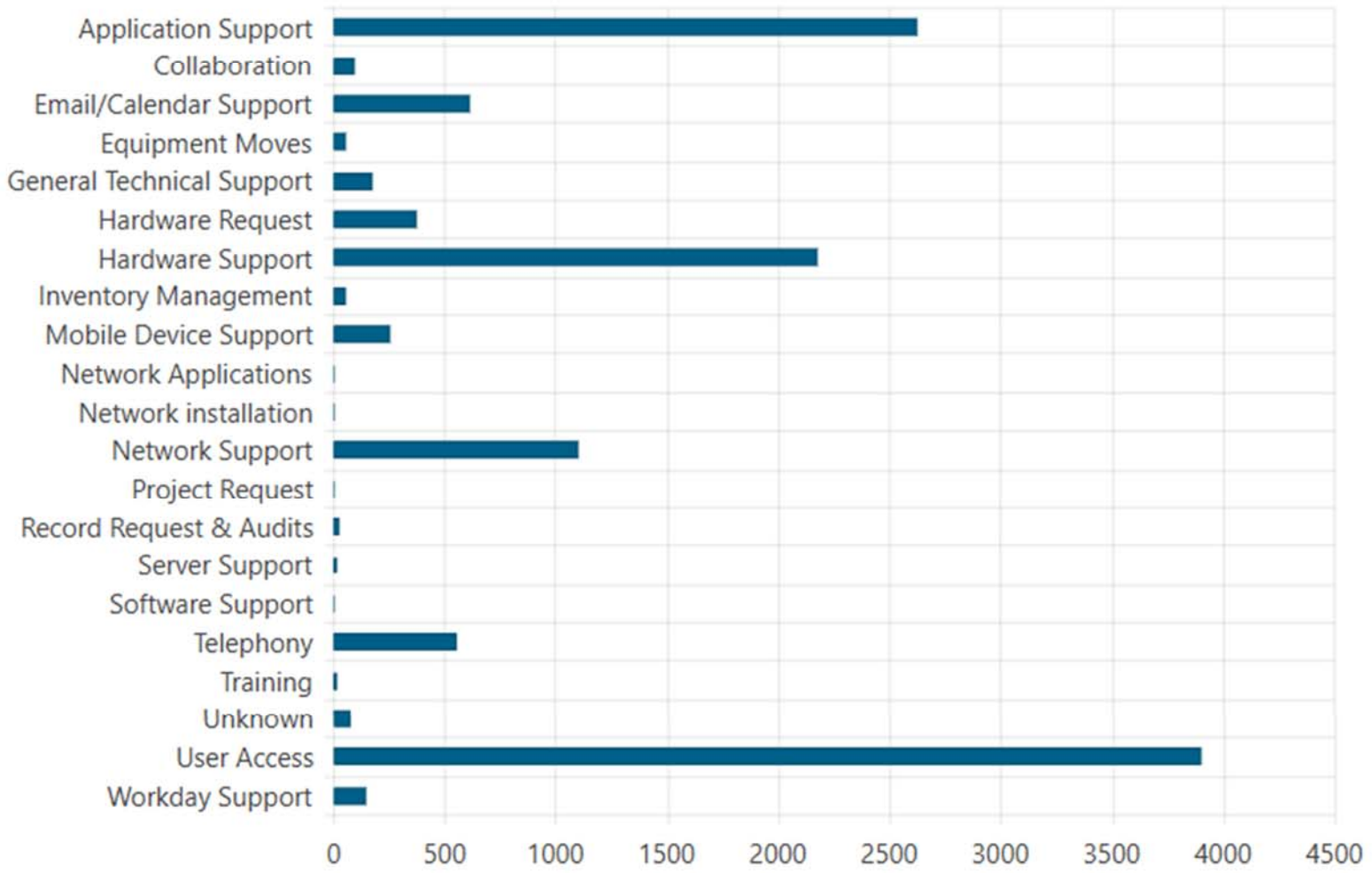
Marathon County - 4,255 North Central Health... - 3,738 City of Wausau - 1,698
City-County Informat... - 1,553 - 362 Everest Metro PD - 92 Rothschild Police - 51
County Credit Union - 38 CCITC - 33 All Others - 185

On Call Entity Year to Date



North Central Health... - 274 Marathon County - 79 City-County Informat... - 39
City of Wausau - 37 Everest Metro PD - 22 North Central Health... - 11
Athens PD - 10 - 6 Mosinee PD - 3 All Others - 14

Tickets Year to Date type



Tickets Year to Date - This chart shows a historical graph of the number of tickets each month since the beginning of the year

On Call Tickets Year to Date- This chart shows a historical graph of the number of on call tickets each month since the beginning of the year

Tickets by Entity Year to Date- This chart shows the percentage of all tickets by entity excluding on call

On Call Entity Year to Date- This chart shows the percentage of on call tickets by entity

Tickets Year to Date Type – This chart shows the tickets year to date sorted by type of ticket

INFORMATION SECURITY PROGRAM PLAN

City-County IT Commission (CCITC)

Table of Contents

1.0 Introduction

1.1 Overview

This policy is authorized and in use by City-County Information Technology Commission, hereafter referred to as CCITC, as defined in the definition page of this document, and it applies to personnel, as defined in the definition page of this document. The confidentiality, integrity, and availability of information stored within and transmitted across the information systems and networks of CCITC must be protected to comply with federal and state law, governing policies, and to preserve our reputation as a caretaker of sensitive information. The Information and Cybersecurity Program defines the governing framework and structure required to support CCITC's security infrastructure and operations.

1.2 Purpose

The purpose of this policy is to establish the governing framework and structure of CCITC's Information and Cybersecurity Program. The goal of which is to protect the confidentiality, integrity, and availability of information systems and data created, maintained, or managed by CCITC by defining the organizational and resource requirements that support the implementation of adequate technical, procedural, and behavioral controls.

1.3 Scope

This policy applies to all personnel (i.e., contractors, and applicable third-party) that manage, maintain, operate or access CCITC's information systems, networks, and data.

2.0 Information and Cybersecurity Program Planning Policies

2.1 (PM-1) Information Security Program

CCITC shall develop, distribute, and maintain an organization-wide information security program plan that:

- Provides an overview of the security program, including descriptions of both the management and common controls implemented or planned to be implemented to support program requirements.
- Includes the identification and assignment of roles, responsibilities, management oversight, coordination among CCITC entities, and compliance.
- Reflects coordination among CCITC business units, management teams, and personnel responsible for activities in support of information security (i.e., technical, physical, personnel, cyber-physical).
- Is approved by CCITC's Information Security Manager, who is both responsible and accountable for the inherent risk incurred by ongoing business operations that are supported by information and communication technologies.
- Shall be reviewed and updated at least annually, as deemed appropriate, to address changes identified during ongoing plan implementation, operation, maintenance, and risk assessments.
- Is protected from unauthorized disclosure and modification.

2.2 (PM-2) Information and Cybersecurity Manager

CCITC shall appoint an Information Security Manager who is charged with the mission of identifying, justifying, and acquiring resources that support the coordination, development, implementation, and maintenance of an organization-wide information security program.

2.3 (PM-3) Information Security Resources

The CCITC Board of Directors shall ensure that proposed information security budgets and requested resources are reviewed and approved, as deemed appropriate and in alignment with CCITC's defined risk appetite statement, IT Strategic Plan, and each supported entities' Strategic Plan.

The Information Security Manager shall:

- Ensure that all capital planning and investment requests detail resources required to implement the information security program and documents all exceptions to this requirement.
- Employ a business plan to record the resources required.

2.4 (PM-4) Plan of Action and Milestones Process

The Information Security Manager shall implement a process for ensuring a Plan Of Action and Milestones (POA&M) is developed and maintained for the security program and associated information systems. This process and associated deliverables include:

- Document remedial actions and activities that adequately respond and reduce risk inherent to the use of information technology in support of business operations, assets, employees, customers, and other resources.
- Ensure reporting requirements are met in accordance with applicable state and federal law.
- Regular review for consistency with formally and informally documented organization-wide risk management strategy, priorities, and response actions.

2.5 (PM-5) Information System Inventory

CCITC Information Technology Staff shall develop and maintain an inventory of its information systems, as well as associated hardware, software, and components. It shall be updated regularly as part of standard and defined information technology management procedures and management activities to ensure all assets to be protected are identified and classified as appropriately based on risk.

2.6 (PM-6) Information Security Measures of Performance

The Information Security Manager shall be responsible for the development of appropriate metrics, systems, and procedures for monitoring the performance of controls implemented for the purpose of mitigating risk inherent to the implementation and operation of information technology systems and networks. Information Security Program performance and metrics shall be reported to the CCITC BOD as defined by supporting programs.

2.7 (PM-7) Enterprise Architecture

The Information Security Manager shall support a security first approach with respect to the development and implementation of enterprise architecture. This approach must consider the inherent risk of implementing new technologies, as well as making changes and modifications to existing information systems.

2.8 (PM-8) Critical Infrastructure Plan

The Information Security Manager shall address information and cybersecurity related issues in the development, documentation, enhancement and retirement of a critical infrastructure and key resources. This includes the development of a protection plan that prioritizes critical information systems, assets, and data.

2.9 (PM-9) Risk Management Strategy

The Information Security Manager shall develop a comprehensive strategy and management program for identifying, measuring, and mitigating inherent risk to CCITC business operations, assets, employees, customers, and other resources associated with the operation and use of information systems. This strategy and program shall be:

1. Implemented and enforced consistently across the organization.

2. Express the organization's risk appetite regarding matters of information security and privacy.
3. Acceptable methodologies and strategies for identifying, cataloging and assessing risk.
4. Reviewed and updated at least annually.
5. Updated as deemed appropriate due to environmental, technological, or procedural change.
6. Aligned with strategic, operational, and budgetary planning exercises and processes.

2.10 (PM-10) Security Authorization Process

The Information Security Manager shall formalize and support the development of security authorization processes that support granting, maintaining, and removing access to all CCITC information systems and networks by both internal and external users. These processes shall define and assign specific roles and responsibilities for documenting, approving, and managing user access. Security authorization processes shall be integrated into the organization-wide risk management program.

2.11 (PM-11) Mission/Business Process Definition

When defining mission/business processes, the Information Security Manager and Executive Management Team shall consider associated information and cybersecurity risk inherent with the implementation and operation of information technology systems and assets. Processes shall be developed with the protection of operations, assets, employees, customers, and other resources prioritized. Processes shall be revised, as necessary, until achievable protection needs are obtained in alignment with the organization's defined risk appetite statement.

2.12 (PM-12) Insider Threat Program

The Information Security Manager shall develop and support the implementation of an insider threat program, designed to identify malicious actors, and intervene before a hostile or harmful act is committed. This program shall support the implementation of controls that

1. Conduct host-based user monitoring
2. Provide insider threat awareness training
3. Support Incident Response Planning and Preparedness efforts

2.13 (PM-13) Information Security Workforce

The Information Security Manager shall establish an information security workforce development and improvement program. This includes:

1. Defining knowledge, skills, and abilities needed to perform security and privacy duties and tasks.
2. Developing role-based training programs for individuals assigned security and privacy roles and responsibilities.
3. Providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions.
4. Including career paths encouraging professionals to advance in the areas of security and privacy.
5. Ensuring positions responsible for maintaining security and privacy are filled with qualified personnel.

Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs. They focus on developing and standardizing of personnel needed to protect organizational operations, assets, employees, and customers.

2.14 (PM-14) Testing, Training, and Monitoring

The Information Security Manager shall implement a process and program for conducting security testing, training, and monitoring activities that support educating the organization’s

workforce on the latest cybersecurity hygiene best practices and red flags. These programs must ensure training programs:

- Are developed, maintained, and continuously operated.
- Continue to be executed in a timely manner.
- Are relevant to employee cyber hygiene responsibilities and current threat trends

The Information Security Manager shall review testing, training, and monitoring plans for consistency and alignment with the CCITC risk management strategy and organization-wide priorities for mitigating risk.

2.15 (PM-15) Security and Privacy Groups and Associations

The Information Security Manager and Information Technology Staff shall establish relationships with selected groups and associations within the security community:

- To facilitate ongoing security education and training for CCITC personnel.
- To maintain currency with recommended security practices, techniques, and technologies.
- To share current security-related information including threats, vulnerabilities, and incidents.

2.16 (PM-16) Threat Awareness Program

Due to the constantly changing nature and complexity of adversaries and attacks, it is becoming increasingly difficult to detect and respond to security threats. The Information Security Manager shall implement a threat intelligence and awareness program that includes cross-organizational information-sharing capability.

3.0 Train Personnel

Personnel are informed by a CCITC Human Resources representative of this policy during the new-hire onboarding process and are incrementally informed when the policy changes.

4.0 Compliance

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Annual Review

This policy must be reviewed and updated at least annually, or as required due to environmental, organizational, procedural, or technological change.

6.0 Policy Exceptions

Any exception to this policy must be reviewed, approved, and documented by the Information Security Manager or appointed personnel.

7.0 Other Applicable Policies

To be completed in 2024

- Acceptable Use Policy
- Access Control Policy
- Identification and Authentication Policy
- Disaster Recovery and Business Continuity Plan (DRBCP)
- Configuration Management Policy
- Remote Work and Telecommuting Policy
- Asset Management Policy
- Security Awareness and Training Policy

To be updated and/or completed in 2025

- Encryption Policy
- Data Protection and Privacy Policy
- Network Security Policy
- Incident Response Policy
- Vendor and Third-Party Security Policy
- Removable Media Protection Policy

8.0 References

- NIST 800-53 revision 5

9.0 Document Change History

Date	Filename/Version	Author	Revision Description