POLICY No. 2010-03

Information Technology Security

Originating Department	CS-IS-01-2010		
SMT Approval:	2010-03-11		
Council in Committee:	2010-05-03	**Recommendation #:**	25
Council Approval:	2010-05-10	**Resolution #:**	114 -10
Revision History:	Click here for revision history		

1. PURPOSE

Information and the systems, networks, and software necessary for processing are essential County assets that must be appropriately protected against all forms of unauthorized access, use, disclosure, or modification. Security and controls for County information and associated information technology (IT) assets which are owned, managed, operated, maintained, or in the custody or proprietorship of the County or non-County entities must be implemented to help ensure privacy and confidentiality, data integrity, availability, accountability, and appropriate use.

The purpose of this policy is to:

- Effectively manage the risk of security exposure within technology systems,
- Establish clear responsibility and authority for protecting information assets,
- Ensure operational continuity, minimize damage to information assets and technology systems from security incidents,
- Alert users in their responsibility for protecting information assets,
- Ensure that this policy, along with the Corporation's IT Acceptable Usage Policy, the IT Disaster Recovery and Business Continuity Policy, and the IT Backup and Data Recovery Policy, combine to create a comprehensive policy framework for protecting information assets and technology systems.

2. POLICY

2.1. *Overview:* This policy deals with the following domains of security:

- Physical and Systems Security
- Data Security
- Network Security
- Operational Security
- Personnel Security.

2.2. *Physical and Systems Security:* Information technology systems are vulnerable to improper or unauthorized access as well as physical assault or damage. Because of the importance of IT resources, and their centralized nature, particular attention must be paid to addressing the requirements for secure systems.

2.2.1. Physical and Infrastructure Security – Equipment will be physically protected from security threats and environmental hazards to prevent loss, damage, or compromise of assets and interruption to corporate systems.

Appropriate measures must be taken to ensure that physical access to data centers and computer server rooms is available only to those individuals who require it to perform their duties.

2.2.2. Systems Security – Processes and controls must be in place to ensure that servers, personal computer systems and application software are protected against unauthorized use or modification, either accidental or intentional.

- Controls are required to ensure that physical access to a server or personal computer system that is connected to the enterprise network is not sufficient by itself to provide access to the system.
- Once a user has the authority to access a server or personal computer, there must be further specific controls on what each user is authorized to do based on the user's responsibilities.
- For server and host computer systems, the Information Systems (I.S.) Division must control user identification and authentication controls and user connection access.
- Although users may be assigned their own personal computers to access the system, they remain County property. When there is a request to upgrade hardware, systems and application software and it is approved by management and I.S. staff, all upgrades must be performed or overseen by trained personnel with the skills needed to plan and implement the upgrades, troubleshoot any problems encountered, and call off the upgrades if required. The I.S. staff can then ensure that only approved, authorized, and licensed software and tested upgrades are installed on each system. Only I.S. Division staff may install or update any system software, application software, or hardware (refer to "01-08 IT Acceptable Usage Policy" for further information).

2.2.3. User Identification and Passwords – Processes and controls must be in place to ensure that only employees who need access to enterprise systems, applications, and data in their daily business duties have that access. These controls require a user to be identified and to confirm this through a password.

- Access to a host computer system, network server, or networked personal computer must be approved by the user's manager who must complete and forward a Checklist – Resources and Equipment form to the I.S. Division.
- Passwords must be used to control system and data access and provide for user authentication.
- Passwords must not be divulged or shared with anyone including other County staff.
- Passwords must be changed periodically and stored securely.

Further, if any activity on the system is auditable, that activity must also be attributed to the individual who bears sole responsibility for the activity.

2.2.4. Confidentiality and Privacy – Confidentiality and privacy must be maintained in order to protect enterprise, supplier, customer and employee information, and to comply with federal and provincial legislation. IT systems and controls must facilitate the corporation's processes and policies to protect confidential information.

IT systems have the ability to store – or release – huge quantities of proprietary or confidential information, so controlling and maintaining confidentiality is vital.

- Haldimand County will take all responsible steps to maintain the confidentiality of information stored on its systems
- Haldimand County and its employees will respect and protect the privacy of personal information.

2.2.5. Controls for Viruses, Worms and Malware – Controls must be implemented to lower the risk against these and similar types of attacks.

- Haldimand County's network will be defended by a firewall and/or filtering device against unwanted intrusion from the public Internet and against unauthorized communications from inside the firewall to the public Internet.
- All computer systems will be protected against malware infections with anti-virus software (AVS) and be updated with the latest AVS protection on a periodic basis coinciding with the AVS-vendor update schedule.
- All programs, files, documents and e-mails from an external source will be automatically scanned for malware infection by the AVS before storage and use.

2.3. *Data Security:* Processes and controls must be in place to ensure that data is secure against inappropriate access, modification, and destruction. The extent to which controls must be in place depends on the characteristics of the data, its value to the corporation, its sensitivity to inappropriate disclosure or modification, and privacy and financial issues associated with the data.

2.3.1. Data Ownership – All system users who create data or are the primary stakeholders in defining application data are owners of the data and must identify their ownership of the data.

2.3.2. Data Access Controls – Processes and controls must be in place to ensure that access to data is restricted in a manner that is consistent with its security requirements.

Several tools and methods are used to restrict both access to data and the type of access granted. Types of access may include the following operations:

- Reading data
- Modifying or updating data
- Appending or adding to data
- Deleting data

Users may access data to which they are authorized, but must do so using authorized applications, programs, interfaces and procedures.

Internal controls must be in place to ensure data owners consult with "experts" in the areas of Freedom of Information, financial, and risk management to ensure that the business processes in place adhere to other policies and legislation.

2.3.3. Application Security controls – Applications provide access to data and the capability to modify or update data. These applications must also include controls to validate the authority of the user and respect restrictions on what data may be updated and to what extent. Appropriate controls, including user access restrictions, shall be implemented and enforced for all applications.

2.3.4. Data Disposal – Security issues extend to media and data that has become obsolete and discarded. For reasons of confidentiality and privacy, data must be disposed of in a secure manner.

2.3.5. Removable Media – Removable media have many uses, not all of which are acceptable for business purposes. Removable media are inexpensive, readily available and easy to use. Data may be transferred between computer systems and removable media at high speed and in large volumes.

One such tiny device can easily hold tens of thousands of data files. Thus there are real security risks associated with allowing the use of removable media in a company.

Risks associated with removable media will be minimized by:

- Authorizing the use of specific removable media only to those users who document their need for this capability and get approval from their manager and I.S. for attaching these to corporate IT systems.
- Directing users on appropriate usage of removable media, including:
  a) Encryption and/or password protection of sensitive data
  b) Appropriate physical handling of media
  c) Keep the removable media stored in an appropriately secure environment that avoids exposure to unauthorized persons, media loss or corruption from external influences such as heat, moisture and electrical or magnetic interference
  d) Send the removable media to the I.S. Division before reallocation or for disposal of the media
- Ensuring that the removable media is not the only place where data maintained for work purposes is stored
- Automatically performing a virus scan of media when accessed
- Logging instances of users connecting removable media
- Implementing active controls as to who can connect what portable media devices to company IT systems.

Information that has been approved for public release can be copied onto removable media such as CDs for distribution to external parties such as consultants, general public and the media.

As per the *Personal Health Information Protection Act* (PHIPA) Order HO-007 from the Information & Privacy Commissioner of Ontario, all mobile devices which contain personal health information must be encrypted. Mobile devices may include, but are not limited to computer laptops, tablets and removable devices, including USB keys.

2.4. *Network Security:* The corporate network is the backbone of the modern IT system. There is a constant conflict between the need to maximize security and control by strictly monitoring and controlling the devices connected to the network, versus the desire to facilitate productivity by allowing such access. The following deal with the control of outside equipment and users accessing the network.

2.4.1. Network Hardware Connection – Processes and controls must be in place to ensure equipment connected to the network does not endanger system security. Therefore, there must be controls over the connection of equipment that is not supplied by the County to the network.

- Direct connection of computer equipment to the corporate network is restricted to County owned and supplied computers and devices with a system image or configuration as defined and maintained by the I.S. Division.
- Direct connection of personally-owned computers or other devices (e.g., laptops, Personal Digital Assistants, cell phones, cameras, USB devices, printers) to the corporate network is not allowed; however, these can be connected to defined access points that are external to the secure internal company network (ie. the “Library Public Access” portion of the County’s network).

2.4.2. Firewall Protection – Processes and controls must be put in place to ensure that firewall systems are established and configured to maximize the protection provided to the network while permitting required access.

Establishing Internet connectivity for an enterprise network creates an external access point to the internal corporate network infrastructure. It is essential that such access be controlled and managed to minimize the risk of unauthorized access and interference to the network, corporate applications and all computer systems.

- All Countynetworks must be designed, configured, tested, and implemented with appropriate and current firewall and/or filtering protection systems.
- Servers, computers, and other devices (if applicable) must have firewall protection installed and configured to limit network traffic to only those protocols or traffic required for business processes.

2.4.3. Remote Access – Processes and controls must be in place to ensure that remote access to the County’s systems, network, data, applications and other I.T. devices is implemented in a manner that minimizes the threat of loss or damage to the corporation’s IT resources and data.

- Remote access mechanisms may be implemented to access corporate internal systems, networks, and data only if:
  a) Remote access can be justified to achieve a business or operational goal;
  b) Remote access can be implemented with sufficient security to minimize the risks of exposing County systems, networks, applications, data and other I.T. devices.
- Remote access may be granted only to those users who have a business need to connect from an offsite location. All users must be approved by their managers.

2.4.4. Wireless Access – Processes and controls must be in place to ensure that the corporate wireless network is configured and operated in a manner that minimizes the threat of loss or damage to the corporate IT resources and data.

- Wireless network connectivity must be implemented using industry-best standards, precautions and setup parameters with respect to security.
- When wireless network connectivity is implemented, the I.S. Division must re-evaluate security risks with respect to known security exposures. This evaluation may result in:
  a) Suspension of wireless support until the risk can be reduced;
  b) Implementation of additional restrictions on wireless connectivity;

c) Implementation of new hardware and/or software to lessen or eliminate new risks.

- Users employing County supplied devices that are enabled for wireless connection to the corporate administration network, including but not restricted to personal computers, laptops, printers, personal digital assistants (PDAs), Blackberries and cell phones that rely on wireless network connectivity, must observe all rules for preventing unauthorized access to the network, preventing unauthorized use or loss of the devices themselves, and the mandatory use of passwords and authentication appliances.
- Wireless access points available at Public Library Branches are attached to a network separated from the corporate administration network. Users accessing the Internet through a library wireless connection will be prompted to agree to Haldimand County Public Library's Internet and Computer Acceptable Use Policy before proceeding to connect to the Internet.

2.4.5. Network Intrusion Detection and Prevention – Processes and controls must be in place to ensure that the County's network is monitored and periodically scanned for unauthorized network intrusions to minimize threat of loss or damage to the IT resources and data.

- Monitoring will be done using industry-best hardware and software that logs attempts to breach the network and analyzes network access logs and connection patterns to identify and log possible breaches for further investigation.
- The monitoring system will detect network intrusions and will react, in real-time, to block or prevent those activities.

2.4.6. E-mail Security – Processes and controls must be in place to ensure that the risk presented by e-mail systems and e-mail messages with respect to loss, disclosure, corruption or damage to the County's network or data is minimized.

- Antivirus software approved for County use must include proactive scanning of e-mail attachments to detect software viruses before email is delivered.
- Industry-standard hardware and/or software approved for County use will be in place to filter out messaging threats including illegitimate spam and viruses.

2.4.7. Electronic Commerce – All electronic commerce applications must have additional processes and controls in place to protect the corporation and its customers against the inherent risks of enabling financial transactions across a public network such as the Internet.

The Payment Card Industry (PCI) Data Security Standard (DSS) represents a set of fundamental security requirements, industry tools and measurements that address the handling of cardholder information. The County must ensure PCI compliance.

2.5. *Operational Security:*

2.5.1. IT Security Audits: Audits, reviews and inspections are methods of measuring the success of an IT security program, and will be used to determine where IT security policies, standards, guidelines, and/or procedures, including security awareness and training, require augmentation, revision or adjustment.

The I.S. Division will conduct assessments of the corporate technology systems security to ensure they comply with the IT Security Policy. The

assessments will be conducted annually and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). The nature of the information asset or system will determine the external or internal reviews required.

2.5.2. Availability and Continuity: Measures must be taken to provide high availability and continuity of the corporate technology systems and information assets, and the processes necessary to perform normal business. Refer to Policy "09-03 Information Technology Disaster Recovery and Business Continuity" and Policy "09-05 Information Technology Backup and Data Recovery" for details.

2.5.3. Externally Developed or Hosted Systems: Externally developed or hosted software or systems must have features that allow the implementation of security controls to comply with the Information Security Policy.

Organizations that host systems or data on behalf of the Corporation must use security controls that comply with the Information Security Policy.

2.5.4. Secure Disposal of Equipment and Media: Devices containing the Corporation's information must be wiped clean with no reasonable means of recovery prior to their disposal.

All equipment containing storage media (e.g. fixed hard disks, tapes, etc.) must be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal. This includes devices with flash memory storage such as Blackberries, cellular phones, USB drives, and PDAs. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

2.5.5. Reporting and Investigating Security Incidents – All security issues and weaknesses should be reported to the Information Systems Division as soon as possible. All security issues and weaknesses will be investigated and the cause and impact will be determined so that it can be avoided in the future

2.6. *Personnel Security:*

2.6.1. Criminal Reference Check – A Criminal Reference Check must be provided by employees identified in Policy "09-01 Criminal Reference Check".

2.6.2. Employee Awareness and Training – All individuals who access the Corporation's Information Assets must be educated on the Information Security Policy and provided with ongoing awareness and training. The aim of security awareness and training is to support the achievement and maintenance of IT security for all Haldimand County systems and services that require safeguards and assurance. It will provide managers, IT staff, technology users, and council members with the requisite skills and knowledge to permit each to carry out IT security responsibilities effectively. Security awareness and training will include assistance to managers and users in ensuring that IT security policies, standards and other documentation are available in a variety of media to all users.

2.6.3. System Access and Acceptable Use – All users must restrict their use of IT systems to those activities deemed acceptable, which are those broadly defined as business use to further the interests of the corporation. Refer to Policy "01-08 Information Technology Acceptable Usage Policy" for details.

2.6.4. Social Engineering – In computer security, social engineering refers to an approach to gain access to information, primarily through misrepresentation,

and often relies on the trusting nature of most individuals. For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. Appeals to vanity, appeals to authority, and old-fashioned eavesdropping are typical social engineering techniques.

Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate. Users must think twice every time: is this real, or a trick? If in doubt, they need to inquire!

3. DEFINITIONS

3.1. *Access control:* mechanism by which, depending on the Identification and Authentication of the User, access to data or resources is allowed.

3.2. *Adware:* software that specifically monitors a person's Web surfing and disrupts it by displaying contextual pop-up advertising.

3.3. ***Authentication*: procedure to confirm a User's identity.**

3.4. ***Authorization*: access granted to a User for the use of various resources**

3.5. *Data Centre*: room where computer or network equipment is located.

3.6. *Denial of Service Attack:* A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

3.7. *Encryption*: data encryption refers to mathematical calculations and algorithmic schemes that transform plaintext into cyphertext, a form that is non-readable to unauthorized parties. The recipient of an encrypted message uses a key which triggers the algorithm mechanism to decrypt the data, transforming it to the original plaintext version.

3.8. *Firewall:* refers to hardware or software, or a combination of both, that protects networked computers against hostile intrusion attempts from a connected public network like the Internet. Successful intrusion could compromise data confidentiality or integrity, or result in data corruption or denial of service.

3.9. *Information Assets*: all the categories of electronic information, including records, files and databases, and Information Systems equipment including any software registered or used by the Corporation.

3.10. *Information Security*: protection of the electronic information from non-authorized access, modification, destruction or disclosure (accidental or deliberate).

3.11. *Information Systems*: group of electronic files, programs, supporting media and equipment, including the network and networking devices, used for the storage, transmission, and processing of data and information for business purposes.

3.12. *Malicious Code*: programs or portions of code conceived to cause damage to a system or the information contained in it, or to prevent the system to be used in a normal way.

3.13. *Malware:* is a general term for these and other software programs that are developed for the purpose of doing harm to computers or via computers.

3.14. *Media:* objects on which data can be stored or transferred.

3.15. *Network Intrusion Detection system (NIDS):* A NIDS is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.

3.16. *Password:* refers to a secret alphanumeric value used to authenticate a user to an information technology resource.

3.17. *Personal information:* information that may be attributable to a specific individual, either directly or indirectly, by reference to an identification number or by one or more factors specific to his or her physical, psychological, economic, cultural or social identity. Personal information includes:

- Name, identification numbers
- Employee files, evaluations, comments, disciplinary actions, income, salary history
- Credit records, loan records, existence of a dispute between a consumer and a merchant
- Medical or health information, blood type
- Ethnic origin, religious or philosophical beliefs, political opinions

3.18. *Port Scan:* A port scanner is a software application designed to probe a network host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

3.19. *Privacy:* the rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information.

3.20. *Removable Media*: includes all devices and data media that can have data written to them and subsequently be removed easily from the host computer, thus conferring portability on the data therein. This applies to devices such as:

- Diskettes
- Optical disks (CD/DVD and Blu-ray)
- Tape cartridges
- Flash memory devices (also called jump drives, thumb drives, USB drives, memory keys, USB keys)
- USB/Firewire-attachable data devices, including but not limited to:
    - Hard drives
    - Digital audio and video players (iPod, MP3)
    - Digital cameras
    - Cellular phones
    - Handheld PCs and Personal Digital Assistants (PDAs)
    - Digital picture frames

3.21. *Social Engineering:* The practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection

3.22. *Spyware:* computer software that obtains information from a user's computer without the user's knowledge or consent.

3.23. *User identifier:* refers to a set of characters uniquely identifying an individual for system access. Typically consists of user’s first initial of first name followed by surname.

3.24. *Viruses:* are self-replicating and often destructive computer programs that spread by copying themselves without the users’ knowledge or intervention. They can infect a computer in a manner analogous to a foreign substance infecting a biological entity.

3.25. *Wireless Access Point (WAP):* In computer networking, a WAP is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi,

Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

3.26. *Worm:* is a malicious program that spreads itself by taking advantage of file or network transport features on a computer system that allows it to spread unassisted.

4. RESPONSIBILITIES

4.1. *Information Systems Division*:

4.1.1. I.S. Divisional staff are responsible to:

- Give approval prior to any personnel, including external vendors, entering the server rooms.
- Ensure all servers and backup media are either locked in a secure room, or in a locked box / cabinet.
- Plan, test, and investigate all system hardware and system and standard application software for security controls and exposures. The I.S. Division is also responsible to ensure that all system and application software installed on personal and network systems is authorized, approved and licensed.
- Supply users with user ids and an expired password for first-time access. The I.S. Division is also responsible to change the user's password to a new expired password on the user's request to assist with suspected password compromise and forgotten passwords.
- Manage data access controls as directed by data owners.
- Ensure that the network design incorporates adequate firewall protection at each network access point, system server, and personal computer system.
- Ensure that all network appliances, servers, and personal systems have their firewall applications configured appropriately.
- Ensure that for each remote access mechanism to be implemented, that mechanism is configured to minimize risk to an acceptable level and incorporates adequate controls.
- Design and configure wireless network access to minimize security risks; to remain informed about the latest wireless network threats; and to manage wireless risks as required, including suspending wireless service when security threats are discovered.
- Evaluate and implement hardware and software network intrusion detection tools to: monitor systems and networks for signs of both failed attempts and successful intrusions; act on detected or reported intrusion attempts; and recommend changes to prevent recurrence.
- Ensure that data is backed up and retained according to the Information Technology Backup and Data Recovery Policy.
- Ensure that an appropriate infrastructure (i.e., both hardware and software), is established to support the controls required for electronic commerce.
- Provision of both software and hardware solutions to meet the PHIPA Order HO-007 encryption requirements.

4.1.2. The I.S. Manager is responsible to:

- Ensure the IT Security Policy and Procedures are updated as required.
- Ensure annual security audits are completed.
- Promote security awareness to the users of the County's systems.

- Conduct investigations into any alleged computer or network security compromises, incidents, or problems.

4.2. *Facilities & Parks Operations Division*:

4.2.1. All server rooms must be locked. The Facilities & Parks Operations Division is responsible for the locks and alarm systems ensuring only authorized personnel have access. I.S. Divisional staff must give approval prior to any outside repair personnel (ie. telephone / cable technicians) entering the server rooms.

4.3. *Individuals (Authorized Users):*

4.3.1. Users must protect Corporate technology portable devices such as laptops, handheld digital devices, cell phones and portable storage devices, given the information they contain and their monetary value.

4.3.2. The user is responsible:

- To keep his or her password confidential. No sharing of passwords is allowed.
- To not allow others to use a workstation when logged in with his/her authentication credentials.
- To change his or her password at first use and on a periodic basis.
- To follow password creation guidelines for keeping his or her password confidential.
- For any processing activity attributed to the user identifier.
- To notify the I.S. Division of any suspected password disclosure and suspected user identifier misuse.

4.3.3. All users are responsible to ensure the safety, integrity, security and confidentiality of information.

4.3.4. All users are responsible for ensuring that information supplied to Haldimand County or its agents or representatives may only be disclosed in accordance with the *Municipal Freedom of Information and Protection of Privacy Act,* the *Personal Health Information Protection Act, 2004* or other applicable legislation.

4.3.5. All users are responsible to encrypt all mobile devices which contain personal health information as per PHIPA Order HO-007 from the Information & Privacy Commissioner of Ontario. Mobile devices may include, but are not limited to computer laptops, tablets and removable devices such as USB keys.

4.3.6. All users are responsible to observe the restrictions imposed on the computer systems and other devices that may be connected to the corporate network. Refer to Policy “01-08 Information Technology Acceptable Usage Policy” for details.

4.3.7. Remote access users are responsible to:

- Protect their remote access mechanisms (passwords, appliances, etc.) against unauthorized use.
- Keep personal equipment with remote access capability in secure environments

4.3.8. All users with e-mail capability are responsible to take appropriate documented precautions regarding e-mail and e-mail attachments. Refer to Policy “01-08 Information Technology Acceptable Usage Policy” for e-mail acceptable usage details.

4.4. *Business Units:*

4.4.1. Managers are responsible to inform the I.S. Division regarding their employee status and employee responsibilities that require specific system authority.

4.4.2. It is the responsibility of the direct supervisor / manager to notify the I.S. Division by way of the on-line helpdesk ticket system of the last day of work for a user that has resigned or been terminated. At the end of the day on the last day of work the user's account will be disabled.

4.4.3. Data owners are responsible to identify the proper handling and best practice decisions associated with their data.

4.4.4. Data owners must consult with "experts" in the areas of Freedom of Information, financial, and risk management to ensure business processes adhere to other County policies and legislation.

5. REFERENCES

5.1. *Haldimand County Information Technology Acceptable Usage Policy*

5.2. *Haldimand County Disaster Recovery / Business Continuity Policy*

5.3. *Haldimand County Disaster Recovery / Business Continuity Plan*

5.4. *Haldimand County Backup and Data Recovery Policy*

5.5. *Haldimand County Public Library's Internet and Computer Acceptable Use Policy*

5.6. *Haldimand County Criminal Reference Check Policy*

Revision History:
For C. A. O. Office Use

REVISION HISTORY					
REPORT	**CIC**		**COUNCIL**		**DETAILS**
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	