Information Security Documentation and Policies

eCards

An Electronic Card Company

by Jolina De Jesus; Jorge Delgado; Alejandro Diaz; Brandon Mao on February 19, 2019

Table of Contents

eCards' Contingency Plan

Note: Contingency planning (CP) is made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP).

Purpose

The IT component of Contingency Planning is the process of ensuring that essential information processing functions (such as access to electronic customer records) can be maintained throughout a variety of incidents and emergencies. The Contingency Plan endeavors to protect the confidentiality, integrity, and availability. The purpose of eCards Contingency Plan is to identify essential business operations or functions; the facilities, equipment, records, personnel, and other resources required to perform those functions; and the plans to enable an effective recovery from an event that affects the normal operation of eCards. The purpose of the IT component of the Contingency Plan is to identify and plan for continuity of the critical IT functions and systems that support the essential business operations. IT Contingency Planning must address three types of disruptions:

• Closure of a facility (such as damage to a building);

• Reduced workforce (such as due to pandemic flu); and

• Technological equipment or systems failure (such as IT systems failure).

Scope

The contingency plan must, at a minimum, address the following IT Security requirements:

1. Identify the functional areas essential to business operations.

2. Determine how each situation, such as fire or flood, or a down website would affect these key areas, what actions would be taken and the resources needed for each one.

3. Set goals for the return to essential operations and return to full normal operations.

4. Identify each required process and document each step in the process, what needs to be done, along with the staff and other resources needed to complete the work. Develop plans for each functional area and the organization as a whole.

Contingency Plan Policy

This Contingency Plan complies with the eCards's IT contingency planning policy as follows: The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

eCards will follow these seven key steps for contingency planning:

1. Develop the contingency policy objective statement
2. Conduct a Business Impact Analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Create the contingency plan
6. Conduct testing and training
7. Review and maintenance

Let us review of the steps to better understand how we may be able to meet contingency planning requirements.

Business Impact Analysis

The business impact analysis phase of eCards's continuity planning process allows eCards to identify and prioritize essential functions, and then to conduct a systematic assessment of the resources (people, facilities, equipment, and records) required to support those functions. In addition, the critical steps taken for BIA is to Identify critical business functions, Identify disruption impacts and allowable outage times, Develop recovery priorities

Preventive Controls

Preventive controls like generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance are operational at the time of the disaster. Separation of duties, proper authorization, documenting, and physical control over assets.

Recovery Strategies

This section addresses the procedures to maintain or restore the essential IT services and functions. Recovery after a disaster has occured the plan will implemented which will have the company running as soon as possible. Several copies of the entire network and data should should be stored in different safeguarded location for faster recovery. Disasters or events should be categorized on a scale from low risk to high risk. Depending on the level of risk a certain step should be taken to accondate recovery from the disaster. During recovery the contingency plan will focus on the following Facility Infrastructure, Data Communication, Network Servers, Application Server and System.

Contingency Plan

This will be the procedure that will be taken into effect after a situation has occurred. The designated CPMT will be responsible for managing the Contingency Plan during each of the following three operational periods. The organization will have a contingency plans ready and prepared as possible to react to a disaster situation ensuring that incident response, disaster recovery, and business continuity are taken into account

Testing and Exercising Plan

* Tabletop exercises

* Drills or system tests

* Functional exercises

* Testing the security system

* Exposing company vulnerabilities

Review and Maintenance of Plan

Constant maintenance and updating to the contingency plan are to be done on a bimonthly basis to ensure that the contingency plan is up to date.

Business Impact Analysis Template

We can use this template below to perform our business impact analyses. Organizing all columns into a spreadsheet simplifies the analysis process. This collection of data facilitates the process of identifying the most critical business functions, the financial and operational impact if they are disrupted, strategies to recover them and time frame targets to achieve recovery.

BU Name	Head Count	Process	Priority Ranking	RTO	RPO	Required by

1. Business Unit Name – Self-explanatory.

2. Head Count – Number of full-time staff in the business unit.

3. Process – Brief description of the principal activities the unit performs, e.g., sales, contractor interface, or investor relationship management.

4. Priority Ranking – Subjective ranking of process(es) according to criticality to the business unit.

5. Recovery Time Objective – Time needed to recover the parent process to business almost as usual following a disruption.

6. Recovery Point Objective – Point in time to which process work should be restored following a disruption.

7. Process Depends On – Names of organizations and/or processes the process needs for normal operations.

8. Process Required By – Names of organizations and/or processes that need the process for normal operations.

Preventive controls

A list of threats to critical IT business processes and data must be created. Each threat should be linked to what processes could be interrupted or terminated and what data is vulnerable. Mitigation strategies for preventing and decreasing the impact of the threat should be documented. For example, remote storage of backup data, documentation or tested response alternatives.

Recovery Strategies

Businesses use information technology to quickly and effectively process information. Employees use electronic mail and Voice Over Internet Protocol (VOIP) telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments from one company to another. Servers process information and store large amounts of data. Desktop computers, laptops and wireless devices are used by employees to create, process, manage and communicate information. What do you when your information technology stops working?

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or

malware could be significant. A plan for data backup and restoration of electronic information is essential.

IT Recovery Strategies

Recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.) Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals) Connectivity to a service provider (fiber, cable, wireless, etc.) Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)

Data and restoration

Some business applications cannot tolerate any downtime. They utilize dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. This is a very expensive solution that only larger

companies can afford. However, there are other solutions available for small to medium sized businesses with critical business applications and data to protect.

Internal Recovery Strategies

Many businesses have access to more than one facility. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site and processing can continue.

Vendor Supported Recovery Strategies

There are vendors that can provide “hot sites” for IT disaster recovery. These sites are fully configured data centers with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of disaster or store it at the hot site ready for use.

Data streams, data security services and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client’s system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security.

Developing an IT Disaster Recovery Plan

Businesses should develop an IT disaster recovery plan. It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up.

Identify critical software applications and data and the hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration.

Document the IT disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works.

Data Backup

Businesses generate large amounts of data and data files are changing throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data could result in significant business disruption.

Developing a data backup strategy begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan

Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server can then be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Options for Data Backup

Tapes, cartridges and large capacity USB drives with integrated data backup software are effective means for businesses to backup data. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan. Backups should be stored with the same level of security as the original data.

Many vendors offer online data backup services including storage in the "cloud". This is a cost-effective solution for businesses with an internet connection. Software installed on the client server or computer is automatically backed up.

Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business. The business impact analysis should evaluate the potential for lost data and define the "recovery point objective." Data restoration times should be confirmed and compared with the IT and business function recovery time objectives.

Contingency Training Plan

Training is essential to ensure that everyone knows what to do when there is an emergency, or disruption of business operations. Everyone needs training to become familiar with protective actions for life safety (e.g., evacuation, shelter, shelter-in-place and lockdown). Review protective actions for life safety and conduct evacuation drills ("fire drills") as required by local regulations. Sheltering and lockdown drills should also be conducted. Employees should receive training to become familiar with safety, building security, information security and other loss prevention programs.

Members of emergency response, business continuity and crisis communications teams should be trained so they are familiar with their role and responsibilities as defined within the plans. Team leaders should receive a higher level of training, including incident command system training, so

they can lead their teams. Review applicable regulations to determine training requirements. Records documenting the scope of training, participants, instructor and duration should be maintained.

If emergency response team members administer first aid, CPR or use AEDs, they should receive training to obtain and maintain those certifications. If employees use portable fire extinguishers, fire hoses or other firefighting equipment, they should be trained in accordance with the applicable OSHA regulation. If employees respond to hazardous materials spills, they also require training.

Who needs training?	What training should be provided?
All employees	• Protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown) • Safety, security, and loss prevention programs
Emergency Response Team (evacuation, shelter, shelter-in-place)	• Roles and responsibilities as defined in the plan • Training as required to comply with regulations or maintain certifications (if employees administer first aid, CPR or AED or use fire extinguishers or clean up spills of hazardous chemicals) • Additional training for leaders including incident management

Business Continuity Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management
Crisis Communications Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management • Training for spokespersons

Drills and exercises should also be conducted to validate emergency response, business continuity and crisis communications plans and to evaluate the ability of personnel to carry out their assigned roles and responsibilities.

Testing and Exercising Plan

Testing and exercises should be conducted to evaluate the effectiveness of your preparedness program, make sure employees know what to do and find any missing parts.

- Train personnel; clarify roles and responsibilities
- Reinforce knowledge of procedures, facilities, systems and equipment
- Improve individual performance as well as organizational coordination and communications
- Evaluate policies, plans, procedures and the knowledge and skills of team members
- Reveal weaknesses and resource gaps
- Comply with local laws, codes and regulations
- Gain recognition for the emergency management and business continuity program

Exercises help improve the overall strength of the preparedness program and the ability of team members to perform their roles and to carry out their responsibilities. There are several different types of exercises that can help you to evaluate your program and its capability to protect eCard employees, facilities, business operations, and the environment

Testing

Tests should be conducted to validate that business continuity recovery strategies will work. Tests should also be conducted to verify that systems and equipment perform as designed. Tests can take several forms, including the following:

Component - Individual hardware or software components or groups of related components that are part of protective systems or critical to the operation of the organization are tested.

System - A complete system test is conducted to evaluate the system's compliance with specified requirements. A system test should also include an examination of all processes or procedures related to the system being tested.

Comprehensive - All systems and components that support the plan are tested. An example of a comprehensive test is confirming that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.

Tests of information technology systems and recovery strategies should be conducted in a manner that resembles the everyday work environment. If feasible, an actual test of the components or systems used should be employed. Since tests can potentially be disruptive, tests may be performed on systems that mimic the actual operational conditions.

Inspection, testing and maintenance of building protection systems including fire detection, alarm, warning, communication, employee notification, emergency power supplies, life safety, fire suppression, pollution containment and others should be conducted in accordance with

manufacturers' instructions and regulatory requirements. If a critical warning system or protection system fails, the consequences could be significant.

A test schedule should be developed in accordance with applicable regulations, standards and best practices and designed to meet performance objectives. Records should be maintained.

Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance.

Types of Exercises

There are different types of exercises that can be used to evaluate program plans, procedures and capabilities.

- Walkthroughs, workshops or orientation seminars
- Tabletop exercises
- Functional exercises
- Full-scale exercises

Walkthroughs, workshops and orientation seminars are basic training for team members. They are designed to familiarize team members with emergency response, business continuity and crisis communications plans and their roles and responsibilities as defined in the plans.

Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular

emergency situation. A facilitator guides participants through a discussion of one or more scenarios. The duration of a tabletop exercise depends on the audience, the topic being exercised and the exercise objectives. Many tabletop exercises can be conducted in a few hours, so they are cost-effective tools to validate plans and capabilities.

Functional exercises allow personnel to validate plans and readiness by performing their duties in a simulated operational environment. Activities for a functional exercise are scenario-driven, such as the failure of a critical business function or a specific hazard scenario. Functional exercises are designed to exercise specific team members, procedures and resources (e.g. communications, warning, notifications and equipment set-up).

F**ull-scale exercises** will be as close as possible toreal scale senario and will be a lengthy exercise which will take place on location using, as much as possible, the equipment and personnel that can be called upon in a real event. For this exercise eCards will the participation from local businesses.

Review and Maintenance of Plan

Long-term plan maintenance will be undertaken carefully, planned for in advance and completed according to an established schedule. The Contingency Plan will be reviewed at least annually or whenever any major organization, infrastructure or systems change occurs. The review will include:

- Contingency plans, policies and procedures
- Testing, training and exercising of the Contingency Plan
- Response to real-world contingency events

eCards' IT Incident Response Plan

Incident Response Plan Overview

This document provides some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide eCards support personnel with some guidelines on what to do if they discover a security incident. The term incident in this document is defined as any irregular or adverse event that occurs on any part of the NPSN. Some examples of possible incident categories include: Compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

* You see a strange process running and accumulating a lot of CPU time.

* You have discovered an intruder logged into your system.

* You have discovered a virus has infected your system.

* You have determined that someone from a remote site is trying to penetrate the system.

There are many different security incidents that can occur with assorted severity levels and not all incidents will require focus on each step. However, it is important to be prepared and understand that typically different phases of security incident plan at eCards are as follows:

- Prepare
- Identify
- Contain
- Eradicate
- Recover
- Review

TERMS

Some terms used in this document are:

ISO - Installation Security Officer

CSO - Computer Security Officer

CSA - Computer Security Analyst

LSA - Lead System Analyst

CERT - Computer Emergency Response Team

CIAC - Computer Incident Advisory Capability

AREAS OF RESPONSIBILITY

In many cases, the actions outlined in this guideline will not be performed by a single person on a single system. Many people may be involved during the course of an active security incident which affects several of the eCards systems at one time (i.e., a worm attack). The eCards CSA should always be involved in the investigation of any security incident.

The eCards ISO (put name here), the eCards CSO (put name here) and the eCards CSA (put name here) will act as the incident coordination team for all security-related incidents. In minor incidents, only the CSA will be involved. However, in more severe incidents all three may be involved in the coordination effort. The incident coordination team will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and clean-up are responsible for providing any needed information to members of the incident coordination team.

Any directives given by a member of the incident coordination team will supersede this document.

IMPORTANT CONSIDERATIONS

A computer security incident can occur at anytime of the day or night. Although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be watching their flocks. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident. Providing information to the wrong people could have undesirable side effects.

RELEASE OF INFORMATION

Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. All release of information must be authorized by the eCards ISO or by other people designated by the eCards ISO. All requests for press releases must be forwarded to the Branch or Division level. Also, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be a security officer from another site. All suspicious requests for information (i.e., requests made by callers claiming to be a CSA for another site), should be forwarded to the eCards CSO or Branch level. If there is any doubt about whether you can release a specific piece of information contact the eCards CSO or eCards ISO.

FOLLOW-UP ANALYSIS

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the eCards ISO and distributed to all appropriate personnel.

Prepare:

- In preparing for security incidents several items need to be addressed.
- Incident handling team should include security officers, system analysts and human resources personnel.
- End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
- Contact information is included as an appendix to this document and should be available in hard copy for:
    - Personnel that might assist in handling the incident.
    - Key Partners who may need to be notified
    - Business Owners to make key business decisions.

  - Outside support analysts with security expertise.

- Backups should be taken and tested
- Supplies to assist the team in the event of an incident (sometimes referred to as a Jump Bag)
- An Empty notebook (Through documentation should be done throughout an incident to include hand written notes in a fresh notebook)
- Boot CDs to analyze hard drives and recover passwords
- Petty Cash

Identify:

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Best practices suggests to declare that an incident has occurred when security officers sense that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved in many security incidents to decide what are the goals in handling a particular incident, such as immediate business recovery or forensic examination.

Contain:

Following basic procedures can contain many incidents. Specific procedures will frequently depend on the nature of the incident, as well as the direction of the business owner. Remember that a compromised machine might not present valid data! Steps to consider include:

- Obtain and analyze as much system information as possible including key files and possibly a backup of the compromised machine for later forensic analysis.
- Powering off a machine might lose data and evidence Preferably disconnecting the LAN cable facilitates containment and forensic activity. (Putting the computer in a separate network with a network analyzer might help analyzing network activity.)
- If one machine has been exploited others may be vulnerable. Actions that might be taken on a large scale might include:
  - Download security patches from vendors
  - Update antivirus signatures
  - Cloe firewall ports

- Disable compromised accounts
- Run vulnerability analyzers to see where other vulnerable hosts are
- Change passwords as appropriate.

Eradicate:

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Boot CDs should be used to access data on compromised machines. (Rootkits installed on compromised machines might affect basic system level utilities and discourage use of a compromised host)
- If machine's OS has been compromised it needs to be rebuilt using hardened machines on appropriate platforms.
- Test any backups prior to restore and monitor for a new incident.
- Document everything.
- Recover:

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Retest the system preferably with a variety of end users.
- Consider timing of the return to production.
- Discuss customer notification and their concerns
- Discuss media handling issues
- Continue to monitor for security incidents

HACKER/CRACKER INCIDENTS

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to the NPSN.

Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible.

There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state (see section 3.2.2). The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to a identification and possible criminal conviction (see section 3.2.3). The method used to handle a cracker/hacker incident will be determined by the level of understanding of the risks involved.

Attempted Probes into a System

Incidents of this type would include: repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts.

Identify Problem

Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Log all actions.

Notify eCards CSA

Notify the eCards CSA within 30 minutes. If the eCards CSA can not be reached then notify the eCards CSO or the eCards CSA backup person. The eCards CSA or their backup person will be responsible for notifying other levels of management.

Identify Hacker/Cracker

If the source of the attacks can be identified, then the eCards CSA (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identify of the hacker/cracker. The NIC may be one source for obtaining the name and phone number of the site administrator of the remote site. If the hacker/cracker can be identified, the information should be provided to the eCards CSO or ISO. The eCards CSO or ISO will provide directions on how to proceed, if necessary. Log all actions.

Notify CERT

If the source of the attacks can not be identified, then the eCards CSA will contact the Internet CERT and CIAC teams and provide them with information concerning the attack. ***NOTE -

Release of information must be approved by the eCards ISO or someone he designates. Log all actions.

Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the eCards CSA or CSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

Active Hacker/Cracker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by the eCards ISO or someone he designates (i.e., the eCards CSO). The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

Removal of Hacker/Cracker From the System

Snap-shot the System

Make copies of all audit trail information such as system logs files, the root history files, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snap-shot information on the system. Log all actions.

Lock Out the Hacker

Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. Log all actions.

Restore the System

Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the log book for this incident. Log all actions.

Review:

This phase is to allow eCards to better handle future security incidents. A final report should be written describing the incident and how it was handled using the Incident reporting form. Suggestions for handling future incidents and reworking this document should be included in this report.

INFORM THE APPROPRIATE PEOPLE

Informing the appropriate people is of extreme importance. There are some actions that can only be authorized by the eCards ISO or CSO. eCards also has the responsibility to inform other sites about an incident which may affect them. A list of contacts is provided below. Section 3 discusses who should be called and when for each type of security incident.

Phone numbers for the people below can be obtained from the eCards Operations Manual in the eCards Control Room. Also, the control room analysts can be of help when trying to contact the appropriate people.

Contact Information:

1. Personnel that might assist in handling an incident

   Joseph D. (###-###-####)

2. Key partners who may need to be notified

   Janno A. (###-###-####)

3. Business owners to make key business decisions

   Kirk S. / Diane D. (###-###-####)

4. Outside support analysts with security expertise

   Joris P. (###-###-####)

eCards' Information Security Education, Training, and Awareness Plan

Security Training Overview

The SETA program may consist of different types of cyber security awareness training and education, such as new hire briefings, security awareness briefings, security reminders, emails, general security training, application specific security training, and job specific security training.

Here are some important rules and guidelines of our security planning.

- A summary of our district information security policies must be acknowledged by all employees, board members, contractors, or third parties with access to eCards sensitive information. A summary of our information security policies, to the extent applicable, will be provided to district contractors.
- Our SETA program will include acceptable use training on handling, transmitting, storing and protection of eCards sensitive information.
- Our SETA program will include physical security policies and procedures.
- Our SETA program will include general information security training such as log-on/off procedures, how to initiate a locked screen saver, password management and other procedures for safeguarding against malicious software or threats.
- Our SETA program will include how to recognize and report a potential security incident or threat to the eCards network.
- Our SETA program will provide updates on new or changes to security policies and procedures.

Purpose:

The purpose of this policy is to define our Cyber Security Education, Training, and Awareness (SETA) program for eCards and to allow our employees to have knowledge of the technological

equipment, proper training of security, and protection of confidential assets around the work space.

Goal:

Our goal is to create a computer-friendly environment through cautious and observed training. With the SETA program, our employees are expected to learn, grow, and succeed through this intensive and thoughtful experience.

Applicability/Audience:

This policy applies to all levels of employees, board members, consultants, contractors, temporary personnel, third parties, and the like and, as appropriate, who have access to the eCards Network. In essence, all employees of eCards are required to take part of the SETA program.

Scope:

We understand that, in order to have a successful SETA Program, it is necessary to train all individuals using computer information resources and handling sensitive information on how to protect this information and what is expected of them.

Policy:

This document outlines the SETA Program needed for employees, users and, as appropriate, outside contractors, consultants, vendors, suppliers, etc. to support our information security policies and procedures.

Benefits:

Training strives to produce relevant and needed security skills and competencies. Low cost but high rewards. Increases ability to hold employees accountable for their actions, but raises security awareness level of the organization. and enhances an employee's behavior and attitude towards information security. Provides Due Care with a training plan and Due Diligence through implemented tests and quizzes.

Focus

It is important to remember the proper education of eCards' information security. eCards provides the following general topics recommended for all employees to understand:

- Organization's security awareness policy
- Unauthorized access to systems or facilities
- Awareness of CHD security requirements for different payment environments and where to get information on protecting CHD in organization.
    - Card present environments
    - Card-not-present environments
    - Phone
    - Mail
    - Fax
    - Online/eCommerce
- Password management and controls
- E-mail security practices
- Secure remote control and access practices
- Avoiding malicious software (viruses, spyware, adware)
- Proper browsing practices
- Mobile device security and policies
- Secure use of social media
- Incident reports strategies
- Countering social engineering attacks
    - Physical/In person
    - Phone/Spoofing
    - E-mail/Phishing
    - Instant Messaging
- Physical security
- Firewalls
- DMZ

Security Education

Objective:

At eCards, we strive to enhance the abilities and understandings of our employees. We will offer special certificates and acknowledgements for employees who wish to continue their knowledge and expedition into our information security department.

Notice:

Computer Security training documentation should be maintained through certificates of training or attendance rosters.

Certificate Program:

eCards offers an external certificates program for employees interested in expanding their information security studies. The program roughly 15 weeks. Applications for the course must be sent to the SETA manager

Security Training

Objective:

Assess employees in workshops, course reviews, evaluations, and quizzes to further test our employees of the technological and security equipment around their work space.

NIST SP 800-16:

“Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.”

Types of Training

General Training:

General security training will be provided as part of the new hire orientation and for existing employees on a periodic basis. An acknowledgement of all training will be signed by the employee at the end of the training/orientation. This is generally an in person briefing conducted by the Human Resources Department ("Human Resources") and addresses our information security policies and procedures. Other mean may be used to include but not limited to web based training, online courses, webinars, training provided by third parties, etc. For non-employees, such as contractors, consultants and third parties, security policies may be set by contract.

Application Training:

Application-specific security training may be given on a specific software or web-based application by Human Resources or Information Technology staff. It emphasizes the types of sensitive information that are accessed and processed on the specific application, as well as important access control features to protect and handle eCards sensitive information and contained by the application.

Job Training:

Job-specific security training will be provided to employees who have access to eCards sensitive information.

IR Training:

Information response security training for Information Technology professionals will be provided to Information Technology individuals to know how to react to a possible incident or preventing a threat from becoming an incident. This training helps reduce risk through appropriate training as first responders.

Web Training:

Web-based security training (e.g., security videos and security briefings/presentations on the web) may be utilized to provide security awareness on handling, transmitting and storing sensitive information, including contractors, consultants and outside third parties.

Methods and Approach

Methods:

Along with the various training, eCards will provide additional methods to further enhance the employees' understandings of our information security. Methods can range from the following:

- PowerPoints
- Employee Handbook (Physical and Electronic)
- Staff Meetings
- Videos
- Workshops

Handicap Policy:

All employees, no matter their social or health status, have the right to partake in this training.

eCards will provide alternative routes for delivering the training for any handicapped workers. Deliverables includes audio applicability and visual applicability (PowerPoints). Please refer to the handicap applicability policy page of eCards' website for more information.

Scheduling:

Security awareness briefings for all staff will be done at least annually. Please refer to our work schedule or contact HR for important updates and deadlines.

Course Review and Evaluations:

Throughout the time, we will provide simple assessments to further enhance and evaluate the employees' performance with our technology. Tests will be administered online and will be sent through your employee emails. Tests will be given periodically. Refer to the work calendar for more information.

Security Awareness

Security reminders, such as emails, newsletters, articles, postings will be provided on a regular basis.

Objectives:

At eCards, we believe it is a fundamental task to keep aware of important computer security issues around the environment.

- **For new employees:**

  New and unskilled employees will be encouraged to learn the aspects of information security by bringing awareness to its importance in the workforce.

- **For returning employees:**

  After successful completion of security training assessments, all employees are encouraged to keep information security safety in their minds.

Future Plans/Programs:

Several plans to keep our eCards security in top shape includes the following but not limited to:

- *Educational Videos*: Similarly to live seminars and lectures, eCards will provide active employees with various online videos to provide brief reminders of general security topics. Videos will be given through an employee's email or watched during a staff meeting every first Thursday of every month.
- *Posters*: Posters with motivational images and key terms/words will be posted around the work space. A little reminder to keep information security as one of eCards' top priority. Posters will be changed every month to a different security topic.
- *Newsletters*: Our weekly updated newsletters (found online) are used to update our users on important security changes and notifications.

External Information

How will this benefit all users?

We believe that having a clear understanding of cyber security is an important aspect of today's lives. With this program, we are confident that our reassessment and awareness of security training can help everyone

Compliance:

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

Accountability:

Information Security is responsible for coordinating with the Information Technology and Human Resources departments to ensure that appropriate training material is made available and training is scheduled on a regular basis.

Information Technology and Human Resources are responsible for ensuring that a user acknowledgement has been signed prior to providing access to the eCards network.

Information Technology is responsible for ensuring compliance with this policy and the controls created to safeguard the eCards network. All violations of this policy will be documented and reported to the department manager and senior management for review and appropriate action(s).

Exceptions:

Any updates, changes or exceptions to this policy must be approved by senior management.

Contact Information:

Human Resources Manager: Man G. (###-###-####)

SETA Manager: Brand M. (###-###-####)

Template Reference

https://www.cibhs.org/sites/main/files/file-attachments/thurs_1115_sunset_ballroom_contingency_plan_template.pdf

https://www.cde.state.co.us/dataprivacyandsecurity/securitytrainingpolicy

http://www.acwajpia.com/filecabinet/rmnopw/Security_Awareness_Training_Education_Policy.doc