INFORMATION TECHNOLOGY AND COMMUNICATION COMMITTEE MEETING

WEDNESDAY, JANUARY 8, 2020
4:00 P.M.
MINUTES

MEMBERS PRESENT: Commissioners Brandon Haskell, Rob Piercefield, Brian Droscha, Jeanne Pearl-Wright and Wayne Ridge

MEMBER ABSENT: Commissioner Jane Whitacre

ALSO PRESENT: Commissioner Terrance Augustine; Jeff Parshall and John Fuentes

The January 8, 2020 regular meeting of the Information Technology and Communication Committee was called to order at 4:00 p.m. by Chairperson Haskell.

The Pledge of Allegiance was given by all.

Commissioner Lautzenheiser moved to approve the agenda, as presented. Commissioner Pearl-Wright seconded. Motion carried.

Commissioner Lautzenheiser moved to approve the minutes of the December 4, 2019 meeting, as presented. Commissioner Droscha seconded. Motion carried.

A proposed resolution to approve the security incident response policy was presented and discussed. The policy is the formalization of the process and procedures contained in the Computer Security Incident Response Plan, to be utilized in response to cyber incidents. Discussion held.

Commissioner Droscha moved to recommend approval of the Resolution to approve the Security Incident Response Policy to the Board of Commissioners. Commissioner Lautzenheiser seconded. Motion carried.

An update was provided on the following technology projects: The completion of the phase-out of remaining legacy devices that have the Windows 7 operating system, the transition to Office 365 e-mail and the network infrastructure upgrade project.

There was discussion regarding continuity between written communications sent by the County and courts and information contained on the County website. The need for continued quality control review will be emphasized to officials and department heads.

An overview of the annual results of the County’s employee cyber security training program was provided.

Chairperson Haskell adjourned the meeting at 4:31 p.m.
The next regular meeting of the Information Technology and Communication Committee will be held on Wednesday, February 6, 2020 at 4:00 p.m. in the Board of Commissioners Room of the courthouse located at 1045 Independence Boulevard, Charlotte, MI 48813.

Brandon Haskell, Chairperson
WHEREAS, the Technology Services Department has developed an Security Incident Response Policy as part of a comprehensive Information Security Policy Manual development to achieve compliance with IRS Pub 1075 Guidelines for the receipt and storage of Federal Tax Information (FTI) within the County-operated technology network utilized by the Friend of the Court; and

WHEREAS, the proposed Security Incident Response Policy has been submitted to and reviewed by the Information Technology and Communication Committee; and

WHEREAS, the Information Technology and Communication Committee recommends the approval of the Security Incident Policy as submitted by the Technology Services Department.

NOW, THEREFORE BE IT RESOLVED, that the Board of Commissioners approves the Security Incident Response Policy, effective immediately.

Abstract
This document describes the incident response procedures to security incidents for Eaton County.

Version Number 1.0
Last Revision Date 01/03/2020
Document Reference ISPM22SIRP
Classification Confidential

REVISION HISTORY
*Updates to this table must be made at each revision of this policy.*

<table>
<thead>
<tr>
<th>DATE</th>
<th>AMENDED BY</th>
<th>APPROVED BY</th>
<th>SIGNATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/26/2019</td>
<td>Al Security Team</td>
<td></td>
<td></td>
<td>Initial Draft</td>
</tr>
<tr>
<td>09/27/2019</td>
<td>Eric P. Daley</td>
<td></td>
<td></td>
<td>Department reference changes.</td>
</tr>
<tr>
<td>01/03/2020</td>
<td>Jeff Parshall</td>
<td></td>
<td></td>
<td>Added reference to the Incident Response Plan as working procedural document for actual Incident or event.</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS

1. Overview ............................................................................................................................................................................. 2

1.1. Procedure.................................................................................................................................................................... 2

2. Purpose ............................................................................................................................................................................... 3

3. Scope ................................................................................................................................................................................... 3

4. Policy ................................................................................................................................................................................... 3

5. Definitions ........................................................................................................................................................................... 4
1. OVERVIEW

The escalated number of attacks on corporate networks, fraud, and identity theft over recent years have driven the need for developing an Incident Response Plan (IRP). This is needed to mitigate the risk of a network compromise or consumer identity theft. With the increased concerns about protecting customer’s Non-Public Information (NPI) and punitive damages that are leveraged by the governing agencies for Non-Public Information with the laws and regulations legislated to safeguard Non-Public Information (NPI), it is imperative that organizations develop an IRP to provide a mechanism to effectively detect, efficiently contain and consistently resolve incidents as they occur. The following are some of other benefits of having an incident response capability:

- Provide an efficient mechanism to effectively and efficiently respond to incident so that appropriate measures can be taken to minimize the exposure.
- Develop procedures for handling incident so that evidence obtained during investigation can be presented in a court of law.
- Utilize information derived from handing the incident to better prepare the environment from being attacked in future.

1.1. PROCEDURE

Incidents where customer data is either disclosed to an unauthorized third party, or could reasonably assumed to have been disclosed, requiring notification of affected customers. The following items are considered incidents. This list is not intended to be exhaustive.

- Theft or loss of paper records containing client data, personally identifiable information, or credit card information.
- Theft or loss of electronic media or devices containing client data, personally identifiable information, or credit card information.
- Inadvertent disclosure of confidential information, via unsealed envelopes, improper inserting, email, improper file server use, etc.
- Successful electronic intrusion attempts whether discovered or reported through alerts from monitoring systems.
- Disclosure of data due to improper file processing, or unplanned customer data changes.
- Suspected breaches of physical security, including burglar alarms, fire alarms.
- Poor print quality, leading to illegible information.
- Improper functioning or unavailability of equipment, websites, or other key business services.
- Witnessing an employee not following corporate security policies or procedure.
- Prolonged, unscheduled downtime of production equipment.

If a breach is discovered or suspected, take immediate action as follows:

- If you suspect computer intrusion, remove the affected computer from the network by disconnecting its cable or disabling Wi-Fi. (Do not turn the machine off, log on to it or modify it in any way.)
- If the breach is production related, immediately stop production, identify all records, files, letters, or envelopes that are suspect, and quarantine them. Do not resume production without approval.
• Notify the Incident Response Manager and your supervisor.
• Preserve all logs, data, files, and paper. DO NOT DELETE ANYTHING.

2. PURPOSE

The purpose of an Incident Response Plan is to provide practical guidelines and actionable steps to respond to an incident effectively, efficiently and consistently. It provides a framework to bring resources together in an organized manner to deal with adverse events related to the safety and security of Eaton County’s information and network systems on any Platform or operating system. What constitutes adverse events will be addressed in the Incident Response Plan (IRP) document, it could include but not limited to; malicious code attacks, unauthorized access to the computer systems, unauthorized utilization of Eaton County, hereinafter referred to as County, services, denial of service attacks, general misuse of systems, hoaxes or identity theft. The IRP provide guidelines to detect, contain, analyze, prioritize and handle incidents effectively. This policy points to the IRP as it provides the framework for identifying, reporting, responding to, and remediating (1) the theft, loss or compromise of confidential information, including both customer data and credit card information, and (2) prolonged service interruptions or downtime. These events are collectively known as incidents.

3. SCOPE

This policy is a framework identifier for the IRP document that is a “working” document and is intended to provide a practical guide to the County Incident Response Team that details procedures in the event of an incident. As with any working document, it is recommended that the IRP be periodically reviewed and tested to ensure adequacy and relevance to current business operations.

4. POLICY

The effectiveness of the response during an incident depends in large part on the decisions and actions of the individuals and teams involved in the process and their interaction when responding to an adverse event. One of the first decisions that must be made is to define what the organization considers as an “incident” so that the scope of the term is clear to everyone involved in process. The definition section will also provide the difference between the term “incidents” from an “event”, and lay the groundwork for high-level policies specific to the IRP.

The Incident Response Plan (IRP) will layout the following items:

• Computer Security Incident Response Team (CSIRT) structure
• CSIRT Member Roles and Responsibilities
• External Response Team Roles and Responsibilities
• Outlines How Sharing Information will be disseminated with outside parties
  o Law Enforcement
  o Media
  o Technical Vendors
• Incident Response reporting structure during an incident
• Incident Response Procedures
• Disaster Recovery planning/implementation
• Review & Legal Review
5. DEFINITIONS

Event - An "event" is any observable occurrence in a system and/or network, such as a user retrieving a file from a file share. However, the scope of this document on addresses computer security-related “Adverse Events”, which are events that negatively impact the operation of the computing environment. Examples of adverse events include the system boot sequence, a system crash, and in more extreme circumstances, packets flooding a network during a Denial of Service (DoS) attack. Environmental events such as natural disasters or power outage are not included within the scope of this document.

In reality, events caused by human error (e.g., unintentionally deleting a critical directory and all files contained therein) have proven to be the most costly and disruptive events experienced within most organizations. However, computer security-related events are attracting an increasing amount of attention within the computing community because of increased computer networking and the exposure that this growth has introduced to internally controlled computer systems.

Incident - An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. This could be an adverse event or a pattern of events with negative consequences (e.g. increased costs or downtime). Sometimes incidents may not always impose costs (for example, distribution of pornography or merely violating one’s privacy); however, to the affected organization an incident does represent a confidentiality breach, a compromise of integrity, or the availability or degradation of computerized systems service.

Although the amount of individual exploits is innumerable, for planning purposes, incidents will be classified under the following categories:

- Hacking (Unauthorized Access, Denial of Service)
- Unacceptable Usage
- Denial of Service
- Fraud
- Malicious Code (Virus / Worm / Trojan)
- Other illegal activities

The interaction between an event and an incident involving unauthorized access to or use of County information systems, whether intentional or otherwise, constitutes an incident. Incident handling involves responding to such events where unauthorized access to or use of County information systems:

- Is suspected to be happening
- Is suspected to have happened
- Is known to be happening
- Is known to have happened