Minnesota Counties Computer Cooperative

Incident Response Plan

Implemented on: 04/09/2020

P: (651) 401-4200 • F: (651) 401-4299 • www.mnccc.org
100 Empire Drive Suite 201
Saint Paul, MN 55103

Table of Contents

Section 1: Overview

The function of this document is to outline a standard incident response plan for Minnesota Counties

Computer Cooperative (MnCCC). An incident includes but is not limited to perceived or intended disruption of safety and security of confidential employee and/or user information; malicious behavior to obtain classified or sensitive information; and inappropriate or unauthorized entry into the MCIT building and/or the MnCCC suite. Should a breach of security occur, MnCCC must take corrective action to eliminate vulnerabilities that may have caused it.

DO NOT PANIC. If you are using this document to recover from a disaster, take your time, and think each process out. Do not just do something to be doing it. Remember for each action there is an equal and opposite reaction. The safety of every MnCCC employee in the event of an emergency is of top priority. In a situation where your life is threatened or you are in danger of physical harm, immediately leave the facility. Never place yourself in a dangerous situation or take unnecessary risks.

Section 2: Scope

This document is for the protection of both MnCCC employees and MnCCC users. This includes threats to the individual, a small group or groups, and/or the entire organization. All threats, even perceived, will be handled according to the procedure outlined in this document.

Section 3: Levels of Threat

Each incident will be categorized under a specific level of severity for documentation and response purposes. The levels are outlined as follows:

3A: Green Level This level indicates that there is no need for immediate response or action. This would include but is not limited to, any spam email, fax, phone call, or physical mail received by an employee or user. Examples of this would include junk mail, an automated call, or suspicious text message. The MnCCC Executive Director has the authority to raise the threat level if needed.

3A.1: Time Requirement Incident response time should not exceed five (5) business days

3B: Yellow Level This level indicates that there is a low to moderate need for response or action. This would include but is not limited to, any email, fax, phone call, or physical mail received by an employee or user. Examples of this would be an attempted, yet unsuccessful, phishing attempt or request for a wire transfer of funds. The received information and its sender should be flagged and reviewed by the MnCCC Executive Director, and, if necessary, MnCCC's IT consultant, who can identify when it is safe to proceed.

3B.1: Reporting This level may require at least one (1) report of the incident by the individual(s) involved. This report will be presented at the next scheduled Board meeting

3B.2: Time Requirement Incident response time should not exceed three (3) business days

3C: Red Level This level indicates that there is a high need for response or action. This includes any received information that indicates information has been stolen or is at risk of being stolen. This level also includes all physical threats to the safety, comfort, and wellbeing of any individual involved directly or indirectly with MnCCC. During this level of incident, the MnCCC Executive Director will immediately act and inform any necessary personnel and/or authority that he, she, or they see fit.

3C.1: Reporting This level will require at least one (1) report of the incident by the individual(s) involved. This report will be presented at the next scheduled Board meeting

3C.2: Time Requirement Incident response time should not exceed one (1) business day

3C.3: Employee Disciplinary Action If the threat is posed by an MnCCC employee, he, she, or they will be subject to disciplinary action and/or severance of employment as outlined in the Personnel Procedures handbook, under the discretion of the MnCCC Executive Director and the MnCCC Board

3C.4: Vendor or Member Disciplinary Action If the threat is posed by an MnCCC member or vendor, he, she, or they will be subject to disciplinary action and/or severance of partnership or employment with the MnCCC organization under the discretion of the MnCCC Executive Director and the MnCCC Board

3C.5: Legal Counsel Consultation with a legal company may be necessary at the discretion of the MnCCC Executive Director to pursue further action if needed

3C.6: Contacting CISA and FBI A Certified Information Systems Auditor (CISA) and the FBI will be contacted when a Red Threat incident has occurred. The purpose of contacting these two entities is to begin an investigation, stabilize and secure data, and recover data from a backup

3C.7: MCIT Breach Coverage MnCCC is currently insured under Minnesota Counties Intergovernmental Trust. Under article 3 of the coverage document, "Cyber Suite Coverage", MnCCC is insured for the following: Data Compromise Response Expenses, Computer Attack, Cyber Extortion, Misdirected Payment Fraud, Computer Fraud, Data Compromise Liability, Network Security Liability, and Electronic Media Liability. Some exclusions and limits of coverage apply. MnCCC will meet with MCIT to review breach coverage and the proper point of contact in the event of an incident

	Green Level	Yellow Level	Red Level
sists of	Spam or suspicious email, fax, call, or mail	Spam or suspicious email, fax, call, or mail	Indication of stolen or potentially vulnerable information, and any physical threats to safety
tocol	If action is necessary, response required within 5 business days	If action is necessary, it may require a report to the Board. Response within 3 business days	Response required within 1 business day. Executive Director will take immediate action, including alerting officials and necessary personnel. Requires a report to the Board. Disciplinary action and/or severance of partnerships will be considered and/or implemented. The counsel of Legal, MCIT, CISA, and/or FBI personnel if necessary

Table 1 - Layout of Green, Yellow, and Red Level threats with criteria for each and the corresponding protocol.

Section 4: Types of Incidents and Responses

MnCCC will identify if an incident requires notification to be sent to the user group(s), vendor(s), or entire membership if needed. If necessary, MnCCC will designate a point of contact to release information after working with MnCCC's IT consultant and/or another information security vendor to conduct a comprehensive analysis and remediation of the breach.

There are three (3) major types of incidences outlined in this document, although all threats received

or perceived by an employee and/or user will be considered to the same degree as those listed below.

4A: Perceived or Intended Disruption of Safety and Security of Confidential Employee and/or Company Information Perceived or intended disruption of safety and security of confidential employee and/or user information including threat(s) to the financial integrity of the organization

4A.1: Procedure for Knowledge of Action If an employee and/or user receives information (or has reason to believe) that confidential data and/or MnCCC's fiscal property or services are at risk of being obtained or disrupted by an unauthorized user, or otherwise misused in any way, he, she, or they should immediately contact the MnCCC Executive Director. If the information at risk involves anything of monetary value, the MnCCC Accountant should also be immediately notified. This type would be considered a Yellow Threat

4A.2: Procedure for Witness Action If an employee and/or user receives information that or witnesses confidential data and/or MnCCC's fiscal property has been obtained by an unauthorized user, or otherwise misused in any way, he, she, or they should immediately contact the MnCCC Executive Director who will carry out detection, retention, and securing as he, she, or they see fit, which also includes contacting any necessary personnel and/or authorities. This type would be considered a Red Threat

4B: Malicious Behavior for Coercion Malicious behavior to obtain classified or sensitive information

4B.1: Procedure for Coercion, Bribery, or Other Threat If an employee and/or user feels coerced, bribed, or are at risk of any other form of threatening behavior to respond to or engage with a malicious entity, he, she, or they should immediately contact the MnCCC Executive Director. This type would initially be considered a Yellow Threat but can be raised or lowered at the discretion of the MnCCC Executive Director

4C: Inappropriate or Unauthorized Entry Inappropriate or unauthorized entry into the MCIT building and/or the MnCCC suite

4C.1: Procedure for Non-Emergency Situations All non-emergency situations should be handled with the MnCCC Executive Director and the MCIT Facility Manager, however, the Saint Paul Police Department can be contacted on their non-emergency line at 651-291-1111

4C.2: Procedure for Suspicious Visitor If an employee and/or user sees or encounters a suspicious building visitor, he, she, or they should immediately contact 911, followed by the MnCCC Executive Director and the MCIT Facility Manager (Kevin Coleman, office: 651-363-0350, cell: 612-859-9195). This type would initially be considered a Yellow Threat but can be raised or lowered at the discretion of the MnCCC Executive Director

4C.3: Procedure for Feeling Unsafe If an employee and/or user feels unsafe or insecure at any time, direct action is required, which involves immediately notifying the MnCCC Executive Director followed by the MCIT Facility Manager and any other necessary personnel under the discretion of the MCIT Facility Manager. This type will always be

treated as a Red Threat, no questions asked, and treated according to the incident response plan

4C.4: General Policy for Physical Safety Employees and/or users should work to the best of their ability to avoid the intruder and make themselves as physically safe as possible for any duration of time they see fit

4D: Treatment for Miscellaneous Activity Any other activity that is not listed in this document will be considered by the individuals covered under the scope of this document. Each incident will be reviewed by the MnCCC Executive Director (and MCIT Facility Manager when necessary) to determine the level of threat posed and indicate the proper response

4E: Recovery and Backup Policy To prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster, data must be backed up frequently. This also helps to permit timely restoration of information and business processes, should such events occur, along with managing and securing backup and restoration processes and the media employed in the process. IT will identify problems and take corrective action to reduce any risks associated with failed backups. Random test restores will be done once a quarter to verify that backups have been successful.

4E.1: MnCCC-Owned Data Entire systems are to be backed up no less than once quarterly. Automatic backups for local data should occur no less than once weekly. These backups will be performed under the supervision of Brave North Technology to ensure the security of data and the successful completion of backups. In the event of a system failure or non-catastrophic loss of information, Brave North will advise when to recover data and notify when systems are clear

4E.2: MnCCC-Operated Data All RSVP backups are to be monitored and maintained by IT CS, LLC, who will also store all website and user data. In the event of a system failure or non-catastrophic loss of information, Mark Weber of IT CS, LLC will advise when to recover data and notify when systems are clear. All MnCCC website backups are to be monitored and maintained by Kindem Design: Creative Graphic Design, Web Development, Branding and Illustration, who will also store all website and user data. In the event of a system failure or non-catastrophic loss of information, Jean Kindem of Kindem Design will advise when to recover data and notify when systems are clear

4E.3: Restoration Requests In the event of accidental deletion or corruption of information, requests for restoration of information will be made to either Brave North of IT CS, LLC depending on the nature of information and where it is stored

Section 5: Rights

All MnCCC employees and Board Members have a right to be informed about all incidents that fall under the Yellow and Red Threat level categories unless otherwise indicated that a situation or result be kept confidential for the safety and security of the individual(s) involved. The information is to be kept confidential and used only for incident response purposes. Any employee, user, or Board Member who violates the privacy of anyone involved in an incident is subject to disciplinary action up to and including severance of employment or partnership.

Section 6: Implementation and Practice

6A: Date of Effect This incident response plan will be in effect when it has been acknowledged and fully signed by the MnCCC staff

6B: Quarterly Practice This incident response plan will be discussed and practiced by MnCCC staff and other necessary personnel at least quarterly, beginning on April 9, 2020, which is a date reviewed and agreed upon by the MnCCC staff

6C: Procedure for Proposed Changes Any proposed changes must be reviewed and approved by the MnCCC staff and Executive Board before making permanent changes to this document

Section 7: Acknowledgement

By signing this document, we, the staff of Minnesota Counties Computer Cooperative, acknowledge that we have reviewed and agreed upon the outlined response plan and agree to adhere to its guidelines to the best of our ability, dated April 9, 2020. We acknowledge that it is our responsibility to maintain the integrity of this document and act responsibly for the safety and security of our information and our colleagues. We understand the importance of this document and its guidelines and will accept any disciplinary action implemented should we as individuals decline to abide.

X	X
Lisa Meredith	Mike Fox
X	X
Amanda Beyer	Emily Ladd

P: (651) 401-4200 • F: (651) 401-4299 • www.mnccc.org
100 Empire Drive Suite 201
Saint Paul, MN 55103

Resources

- Brave North Technology is MnCCC's information services provider. They offer quick-response IT support, data security and management, and much more.
    - Website Link: www.bravenorthtech.com
    - Phone Number: 612-412-4606
    - IT Support Desk Email: support@bravenorthtech.com

- IT CS, LLC is MnCCC's programming service provider. They offer custom program and database design, along with server setup for website and IT support.
    - Phone Number: 507-351-5129
    - Email: markw@it-cs.net

- Kindem Design provides creative and programming assistance for MnCCC. The company also works with domain providers to obtain and maintain security certificates to ensure website integrity.
    - Website Link: www.kindemdesign.com
    - Phone Number: 952-240-6356

- Minnesota Counties Intergovernmental Trust is a partner of MnCCC and offers a wide range of insurance for counties and other state agencies, including Data Compromise and Cyber-Attack Coverage.
    - Website Link: www.mcit.org
    - Phone Number: 651-209-6400
    - General Information Email: info@mcit.org

- MnCCC is growing its relationship with the Minnesota Department of Homeland Security and Emergency Management and the Department of Public Safety. The organization also offers several templates for security documents that agencies can use at their disposal.
    - Website Link: dps.mn.gov
    - Phone Number: 651-201-7400
    - Email: dps.hsem@state.mn.us

- Minnesota's FBI headquarters are located in Minneapolis. It is vital to information security and legal practices to alert the FBI in the event of any criminal or fraudulent activity. This office covers the entire states of Minnesota, North Dakota, and South Dakota.
    - Website Link: minneapolis.fbi.gov
    - Phone Number: 763-569-8000

- SecurityStudio offers modern products for risk, compliance, and security leaders to protect critical information. They also offer security assessments and tools to increase organizations' information security.
    - Website Link: www.securitystudio.com
    - Phone Number: 877-758-9540