

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

EMU-CC Physical Security Policy  
Section B

The purpose of this policy is to protect EMU-CC's physical assets from reasonable threat agents.

This policy will require asset protection from natural disasters, potential thieves, saboteurs, untrained/unskilled operators, and unintended events that are both inside and outside of our realm of control. All aspects of this policy will be considered "high priority" unless otherwise noted.

Physical access to all secure, and vital computing/networking areas shall be maintained and controlled by personally indefinable means. All forms of access shall not be shared under any circumstance, and will also be controlled with a "need to access" concept in regards to times, days, and locations. This will allow for us to know who was where when an incident occurs.

All physical assets that are vital to the operation of the network, EMU-CC, or any other networking/computing equipment shall be tagged, and tracked as per the location of where the item should be. All tags shall be non-removable, and permanent. This will help reduce confusion in the audit process, and identification in the event of theft.

Servers, networking equipment, or other electronic devices vital to the operation of EMU-CC, or the network shall be placed in an environmentally secure room with as short a distance from the main network connection as possible.

Servers, networking equipment, or other electronic devices vital to the operation of EMU-CC, or the network shall not be placed on a ground level, or below ground level room, this is to protect against potential flooding and the following damage that may occur.

Servers, networking equipment, or other heat sensitive electronic devices shall be placed in a temperature controlled area to help prevent over-heating.

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

All servers, networking equipment, or other electronic devices vital to the operation of EMU-CC, or the network shall be physically restrained by conventional means. This is to ensure that things that are placed somewhere that are not intended to move around stay in the intended location.

Any and all physical back up media shall be physically secured onsite under controlled access methods.

Any and all physical back up media that is considered high value shall have a secondary copy made to be stored off site of the EMU-CC but still on campus.

All rooms containing vital operational equipment shall be under video surveillance that will be monitored.

In regards to human operators, there shall be 2 operators in the building at all times, one in charge, and one backup. The backup may be assigned to other tasks until they are needed to relieve the operator in charge. The backup may also be chosen from currently available personnel in the building so long as the individual selected has received the proper training, and has proper access and authority to perform the duties that are required.

Any and all cabling that is needed to be done will be done under best practices for current cabling methodology.

Any technology that is EOL and may potentially become a physical hazard shall be replaced at the earliest possible time, and will be used as little as possible until that time is reached.

Guidelines, procedures, standards, and controls will need to be revamped to accommodate the new policies. Please keep in mind that these policies are not bendable and must be observed.

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

Procedurally, the EMU-CC will need to look the scheduling procedures to ensure that 2 operators are on at all times that are needed. They will need to set higher standards as to the cabling practices. Access procedures will need to be enforced and a new access system will need to be installed. They will also have to look into how often the access control method(card, rfid, codes) will need to be changed to ensure accountability. The analyst team will need to assign new rooms for the equipment and ensure that the environmental controls for this room are properly maintained.

#### EMU-CC Network Management Policy Section C

The purpose of this policy is to ensure a stable, reliable environment across the board with in EMU-CC switching room, and computing environment. To ensure that things are the same everywhere you go will ensure that an operator will find it easy to sit down at any computer, and be able to perform his or her tasks as needed. This policy also intends to reduce the risk of infection spreading across the network. By following this policy it will also reduce time in troubleshooting issues that may arise during normal operational times, as well as in an emergency situation. This policy assumes that an incident will occur at some point in the future.

All inside facing, and outside facing machines shall be configured using the appropriate NIST configuration standards. These configuration standards may be adapted as necessary as long as they are approved by the parties in control of making that decision.

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

All machines that are intended for testing, such as virus storage locations, or database servers intended to be attacked, shall be on a private segment and shall never connect to the main network, or the EMU-CC segment. This will ensure the risk of accidental infection will be greatly reduced.

The network will consist of an appropriate layered approach. With a firewall and IPS on the outside of the network, and a firewall and IDS on the inside of the network.

Each computer shall have a personal firewall properly configured on it to control spread of infection, or to prevent unauthorized transmission from third party softwares.

All software will be commercially available and licensed, but software that is considered open source may also be used with the caveat that it has been tested, and the code certified by the appropriate parties.

Anti-virus software will be made an exception from the previous statement, and must come from a highly regarded anti-virus company. The reasoning behind this is to have a reliable team of developers to work with when incidents occur.

Networking technology shall be of the same IOS(Internetworking operating system) type, cross operating systems shall not be used as they are too difficult to securely configure to be able to work together.

Network access control methods should be configured such that any device that connects will have already been physically inspected and certified by the security team for EMU-CC.

Network access will be denied to any machine that has not been certified by the EMU-CC security team.

Any log on request shall be logged by the EMU-CC authentication server whether or not it was approved or denied. Logs for access shall be maintained for no less than one year.

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

Physical configuration of the machines should be secure against unauthorized media.

All networking equipment, servers, and machines shall be insulated from unexpected power fluxuations.

All equipment shall also have a power backup that is capable of handling short term power loss.

Unauthorized media will not be allowed within the EMU-CC or the switching room.

Operating systems shall be in line with current standards of safe computing, but will not adopt operating system technology early under any circumstance until it has been certified by the EMU-CC security team, and NIST.

The guidelines, standards, controls, and procedures that must be reviewed by the EMU-CC analysts will include EMU-CC's current procedure checklist for system configuration. How, and how often penetration tests are done against EMU-CC's systems. Procedure for infection, and incident response in case of something getting in. The backup procedure must also be reviewed in case of catastrophic data loss, operator error, or malicious user. A new procedure for removing data from the EMU-CC must be developed to ensure safe transition from locations and to insulate the network in case the media comes back infected. Network configuration procedures must also be re-examined for segmentation purposes. The EMU-CC Analysts will also have to look at vendors for AV and ensure that they are capable of being contacted within 1 hour of an incident. The EMU-CC Analysts should also look at machine change prevention software and the procedures for changing the static image as needed. They will also need to review the technology standards for networking equipment for the laptop, desktops, and pda's that may be used in the environment. Over all the policy is set in place to be flexible enough to allow for change within but it must be highly monitored change. A new log audit, process must be instituted to regularly check for unauthorized attempts to gain access to the network. The log

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

audit process will require them to look at the logs for both the IDS and IPS more than likely, and will also have to set up a paging system in case of intrusion, or attempted intrusion. A lockdown procedure will have to be created for when an incident occurs.

## Operation Section D

The following plan has been designed for a disaster scenario in which there is a high potential for attacks on important emergency system resources. Projected electronic threats to this system include, but are not limited to the following: remote attacks on personal computers, and server machines, virus, spyware and adware issues resulting from lack of responsible scanning and patching practices, the potential for problems resulting from both electronic failure and sabotage are also identified as potential threats depending on the reason for this emergency scenario to be engaged.

This policy will effectively mitigate any risk coming from a virtual and physical attack during the time that the Eastern Michigan University campus is under emergency lock down. It will mitigate this risk by increasing the difficulty by which a user with malicious intent with the necessary skills would encounter if an attack upon this system is to be terminated.

In the case of an incident in this scenario, emergency response must be notified. In the case of a physical breach, dispatches must be sent immediately to both DPS and the system administrator. In the case of an electronic breach, a notification must immediately be sent to the system administrator.

In the event of a physical incident, the responsibility of securing the building physically falls upon the department of public safety.

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

Patch management will be controlled by the building administrator and must be checked weekly. If any Macintosh computers operate on the network, these updates will be done every Tuesday (as Tuesday is the day that Macintosh releases their patches.)

Testing of the system must comply with all local, state and federal laws. Port scanning in the state of Michigan must be performed locally. Port scanning may not be performed over a network in Michigan. All testing must also be performed by approved and appropriate equipment. Equipment that does not fall into this category can endanger the system and therefore may not be used. The results of these tests are to be stored on a separate system that must follow strict security standards. The results also may not be shared with anyone outside of the administration of the computer system.

System monitoring and auditing will be relegated strictly to the system administrator. Monitoring of certain system segments may be delegated to other skilled individuals at the discretion of the system administrator, but under no circumstance should the auditing of a system be left to anyone except the system administrator, the building administrator, or the Department of Public Safety. All other parties may not be privy to this information.

Important system information must be backed up on multiple RAID disks. The most important information must be backed up on a mirroring RAID disk. Any other information that must be saved multiple times may be backed up in any way as the system administrator sees fit.

Using this simple policy as a basic guideline for detailed policy, I would recommend that development of this policy should concentrate mostly on the possibility of physical attacks. This is not to say that the possibility of electronic attack is any less, but In the event of a catastrophic emergency on the EMU campus, physical equipment must be secured as a primary action in light

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

of an incident. Once the equipment is secured and well maintained, then the electronic security of the machines becomes the primary focus of the system administrator.

## Exchange Section E

This document aims to put a set of standards to the emergency services area for the safety and security of the students, staff, faculty and any other civilians on Eastern Michigan University's campus. Another high priority goal is to protect the equipment being used. By doing this, we will better help secure our people.

Software configurations will be done only by the system administrator. Installed software must be approved and meet programming standards that include clean programming without any coding impurities, and the ability to modify the original code for customization to our needs. These requirements may be elaborated as needed.

Information will be stored in many different places. Redundancy is important especially when working with information that has a high value. The aforementioned information will be redundantly stored on 3 encrypted disks. High priority information such as this will be mirrored and immediately encrypted to avoid theft. Low priority information will be stored on personal computers, and all information from personal computers in each isolated area will be stored to an encrypted disk which all the computers in each individual area will be networked to and backed up with. If space becomes a commodity, then low priority information will be stored with a grandfather, father son system where old information is deleted.

Password policy will follow the same policy as Eastern Michigan University's my.emich password policy which is each user must choose a password that is at least 8 characters long,

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

with at least one number that may not be at the beginning or the end of the password. All new users must be approved by the system administrator and accounts for each of these users will be created with according rights by the system administrator.

Encryption is very important to this operation, and therefore will require high encryption for high priority information, but even the low priority information must be encrypted. All information being stored at the Roosevelt location will be encrypted with the same encryption. This will mask the importance of the software to any intruders to the system remotely.

Information as necessary will be printed out in hard copy format and stored in a locked cabinet in the system administrator's area. To retrieve hard copies of information stored in this cabinet, the user will need to speak with the system administrator to get the information. If there is any other information that will need to be printed out in hard copy format, the user will be allowed to keep it in a personal file cabinet, but this cabinet must be locked at all times when not in use.

Close communication with local law enforcement will need to be made by putting emergency telephone numbers on all telephones in the area. These numbers must include local police, fire and medical. In the case of an emergency, these numbers will be used to summon the correct authorities to assist in the emergency situation. These telephone numbers will be updated once every 6 months or when needed.

Secure communication will be completed by encrypting any emails that need to be sent on or off campus. Landlines must always be used for business regarding the security of the equipment and campus security in general.

This policy is simply a set of easy guidelines to protect the EMU-CC area in the case of an emergency. The procedure, and programs used must be looked at to determine what is

Alex Fernandez-Gatti(B,C), Nick Crose(D,E)

appropriate for use for sensitive and non-sensitive communication. Printing procedures will have to be examined to see if they will allow for checking for what has been printed. Copy machines will also have to be examined to see if they store digital copies of the documents that are copied on them. These rules must be followed closely for the successful security of the EMU campus when an emergency happens.