UNIVERSITY OF
NORTHERN COLORADO

IM&T Compromise Policy for University of Northern Colorado

Purpose

This document outlines the universities policy regarding compromised computers.

Applies To

This Policy applies to all faculty, staff and third-party agents of the University as well as any other University affiliate who is authorized to access Institutional Data. In particular, this policy applies to those who are responsible for classifying and protecting Institutional Data, as defined by the Information Security Roles and Responsibilities.

Definitions

Compromised System – any computer which has been affected by malware, exploit, or unauthorized access.

CIRT - Computer Incident Response Team

Compromise Policy

If it is determined that the system was compromised the incident should be immediately reported to your supervisor to determine if this should generate a CIRT response. If a CIRT response is not required use the following instructions.

The best security practice in the case of a compromise, unless an investigation is required, is to reimage the machine and restore the data from a known good state. When a machine is compromised there is no way to ensure that all malicious activity on that machine is halted without reimaging the machine.

1. Evaluate the access of the user and the information stored or accessible on the system. If the determination is that the system has access to Restricted Data or that the user has elevated privileges that could pose a risk to the institution, please report that to your supervisor to reconsider a CIRT response.

2. Rebuild the compromised device. This includes understanding the timeline of when the incident took place and restoring the backup to the most recent uncompromised state. This is the primary action that should be taken.

3. If the risk is determined to be low and the value of the potential lost data is high a IM&T Assistant Director, Director or Security team member may approve an attempt to remove the virus or reverse the damage done in the compromise. If the Support Services representative evaluates the risk to be high they must respond with the action described above in #2.

4. If the data cannot be restored from backup, an IM&T Assistant Director, Director or Security team member may approve an attempt to transfer the files from the infected machine to a reimaged machine but ONLY if they are confident that the files do not pose any risk of continuing the compromise. If the representative feels that there is a significant risk they must respond with the action described above in #2.

5. If the investigation reveals that system contains Restricted Data the incident should be reported to your supervisor to determine if a CIRT response is required. The Support Services representative should do their best to determine the potential risk of specific infections. If the risk cannot be determined the Office of Information Security should be engaged.

6. If the user's computer suffers from multiple malware infections the local admin privileges will be removed. This will give the institution an additional layer of protection against malware that would cause significant damage using the user's elevated privilege. In addition, this gives the user the ability to identify when, where and how the infections are occurring. The Director or AVP of the effected user's department can ask for an exemption to this if it impacts the user's ability to perform UNC mission critical tasks. The exemption request needs to be documented, reviewed, and approved by an IM&T Assistant Director, Director, or Security team member.

Revision History

Version	Published	Author	Description
1.0	2014/12/10	Matt Langford	Original publication.
1.1	2015/02/10	Matt Langford	Format update. Minor revisions
1.2	2015/05/06	Matt Langford	Department updates. Process updates.
1.3	2015/08/26	Matt Langford	Addition of #5. Added the following: If a CIRT response is not required use the following instructions. Added the evaluate portion of the process.
1.4	2015/09/03	Matt Langford	Added the AD/D and security team interface into the decision tree
1.5	2016/08/17	Matt Langford	Annual review. Minor adjustments to language and the addition of the CIRT definition.
1.6	2017/07/19	Matt Langford	Annual review. Minor revisions. Now requires approval to grant exemption to user who has multiple malware infections.
1.7	2018/06/05	Matt Langford	Annual review. Removed year from footer.