**Inject 1**

Acceptable Usage Policy

Subject: Acceptable Use Policy

The auditors have noted we completely lack any security policies and a proper and enforced

policy is what keeps a company like ours from becoming the next target. I did some quick

checking on the Internet and found plenty of resources, samples and templates. The board

is demanding we get something to them today for their approval.

The policy you create and can be organized and detailed as you like, so long as the policy is

clear enough for our users to understand. At minimum it should address three areas:

1) System Usage Guidelines

2) Allowed Applications on the network

3) Peer to Peer sharing

Please create a draft policy that addresses each of these 3 points, provide best practices,

and address any other areas you deem important. Post the policy somewhere on our web

server so all employees can access it. Upload a document to the Team Portal with a link to

the policy.

I need this done in 60 minutes but I do not expect you to reinvent the wheel. Try and rely on

existing resources. Just make sure you cite any source material copied and make sure you

begin abiding by the policy you recommend. Keep it to 3 pages maximum.

-------------------------------------------------------------------------------------------------------

Accetable usage policy for Our Company:

**1. Overview** Infosec’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Group XX company’s established culture of openness, trust and integrity. Infosec is committed to protecting 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, Peer-to-Peer communication, and FTP, are the property of . These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**2. Purpose** The purpose of this policy is to outline the acceptable use of computer equipment at Group XXX company. These rules are in place to protect the employee and Group XXX company. Inappropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues.

**3. Scope** This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Group XXX company, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Group XXX company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Group XXX company policies and standards, and local laws and regulation.

**4. Policy**

4.1 General Use and Ownership

a. 4.1.1 Group XXX company proprietary information stored on electronic and computing devices whether owned or leased by Group XXX company , the employee or a third party, remains the sole property of Group XXX company. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

b. 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

c. 4.1.3 You may access, use or share Group XXX company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

d. 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

e. 4.1.5 For security and network maintenance purposes, authorized individuals within Group XXX company may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.

f. 4.1.6 Group XXX company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

a. 4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

b. 4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

c. 4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

d. 4.2.4 Postings by employees from a Group XXX company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Group XXX company , unless posting is in the course of business duties.

e. 4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Software and application acceptable usage and licensing

a. Software may only be used in compliance with applicable license and purchasing agreements. Only authorized copying of files or programs and authorized program utilization are ethical and legal. The Information Technologies Department is charged with the responsibility for enforcing software licensing compliance for the Group XXX company. Please refer to the[IT Support Standards](http://www.css.edu/Administration/Information-Technologies/Computing-Policies/IT-Support-Standard.html) for detailed information.

**4.4 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Group XXX company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Group XXX company -owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 System and Network Activities: The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Group XXX company.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Group XXX company or the end user does not have an active license is strictly prohibited.

c. Accessing data, a server or an account for any purpose other than conducting Group XXX company business, even if you have authorized access, is prohibited.

d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

g. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

**4.5 Peer to Peer Policy**

It is the policy of Group XXX company that the company’s network connections may not be used to violate copyright laws. The unauthorized reproduction of copyrighted materials is a serious violation of Group XXX company’s Internet Acceptable Use Policy, as well as U.S. Copyright Laws, as discussed above. In order to ensure compliance with the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and law enforcement, peer-to-peer file sharing has been restricted by the company. All peer-to-peer file sharing network activity will be monitored and usage tracked. Network activity that utilizes peer-to-peer applications that have a high prevalence for distributing copyrighted material will be blocked.

-----------------------------------------------------------------------------------------------------------------

**Inject 2**

Terminated Users

Subject: How do we handle terminating users?

Team, I've got a pending HR issue with some employees and I want to make sure we have a

process in place, if we happen to let them go.

I need you to provide me a list of 10 steps that you will perform to ensure a terminated user

cannot access any of our resources.

All inject responses must be submitted as attachments.

- All text documents must be submitted as PDF files.

---- All other file formats (DOC, DOCX, ODT) will lose points.

- All spreadsheets must be submitted as CSV file format only.

---- All other file formats (XLS, ODS) will lose points.

Submissions without attachments will lose points. If the inject asks for confirmation, Create a

PDF document and submit it to the portal.

All filenames must incorporate the following naming convention: Inject Number, Underscore,

Team Number, File Extension

-------------------------------------------------------------------------------------------------------------------------

Ten Steps:

1. Gain Access to User Account.
2. Backup User System Logs.
3. Delete Logs on User System.
4. Change User password and set the password to not be changed.
5. Remove User from any Groups.
6. Set User account to Disabled.
7. Set the User to ‘Log on to’ to no computers.
8. Set the User’s Properties to ‘NULL’ or ‘Terminated’.
9. Add the User to a Group of Terminated Employees.
10. Remove the User from the Active Directory Domain Controller after a set amount of time.

-------------------------------------------------------------------------------------------------------------------------

**Inject 3**

Disappearing Laptops

It looks like our new hires don't have the magic needed to make it here. We will be

terminating the employment of several users listed below. Please lock their accounts and

provide a report on any activity that was suspicious.

Robert Peters

Joyce Bowman

Audrey Ward

Julio Andrews

Please let us know when the users accounts are locked so HR can have them escorted from

the premisses.

Thanks,

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Deliverable: A PDF with User names and Account status all users listed. Small description of

what steps were taken to ensure that each user did not take any action against our

company. No more than 2 Pages total.

**Inject 4**

Subject: Data Classification and Risk Assessment

You have been hired as part of a team to take on the support of an existing infrastructure. The organization has issued a number of interim security policies that the network needs to be in compliance with. The theft of the organization's intellectual property is a concern and can

cause significant liability in the event of a breach. In particular, the organization is concerned about APTs (Advanced Persistent Threats), caused by end-users falling victim to phishing attacks. Management needs guidance on how to identify and protect various types of information. IT needs to define data classification categories and criteria that, at a minimum, distinguishes corporate proprietary from other types of data.

IT then needs to perform an assessment of what different categories of information are stored, where it is stored, and then define processes to ensure protection of this information. IT will also ensure that all communication with management is labelled appropriately. Incorporate your policy into your operations.

Your deliverable is a copy of your Data Classification Policy that can be added to our overall Corporate Policy Manual.

**Inject 5**

Subject: Hashing

We consider modifications to files a reportable security incident. Please calculate hash values for all the files located on Rey, Dameron, and Hux. Please submit an electronic report of the hashes to the blue team portal.

**Inject 6**

Subject: Plan for system hardening

Team,

It seems we have cut a lucky break. The networking gurus are still making final configurations to the network and most public traffic is being blocked. Our internal users are still depending on system availability but we have 45 minutes of breathing room before any malicious activity. Please prepare a 1 page summary report detailing the actions you are taking to harden our environment.

This report is required for justification of the extra expense (i.e. your consulting fees) and will be going to upper management. Please take the time to make it look professional.

**Inject 7**

Subject: Status Update

You have probably noticed the Red Team has made their presence known. It is not like this is your first time at the picnic. Please provide a report broken into three sections.

Section #1: What steps have you already taken?

Section #2 What immediate steps are you taking in the next 60 minutes?

Section#3: Where are your priorities before the end of the day? What you are looking for and any specific steps or plans you wish to execute?

If necessary, you should include needed performance optimizations or required configuration changes. Please have this done in 90 minutes and remember this is going to our executives. Make it look professional and cite any outside sources.

**Inject 8**

Subject: Security Policy

A proper and enforced security policy can prevent your team from becoming the next sad news story. We started your team off without any such policy, however, a quick check on the Internet and you will find plenty of resources, samples and templates.

Please use these resources to create a policy. The policy you create can be as organized and detailed as you like, so long as it is clear enough for users to understand. At minimum it should address three areas:

1) User Password and System Usage Guidelines

2) Data Loss Prevention

3) Network Change and Configuration Management.

Please create a draft policy that addresses each of these 3 points and provide best practices we should be following. As well as uploading your final document to the Team Portal, with a Post of the policy somewhere on a web server so employees can access it. Include the link for the online version when you submit.