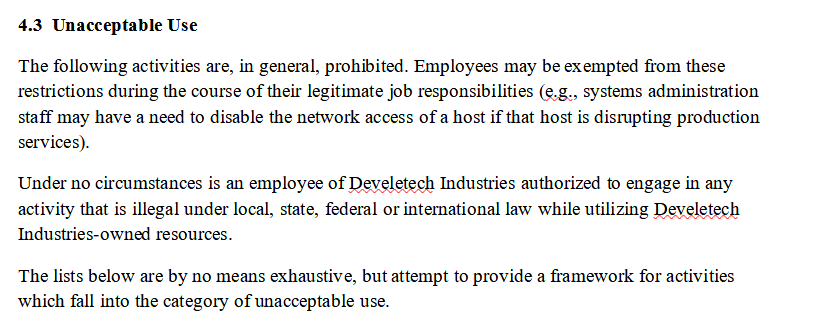
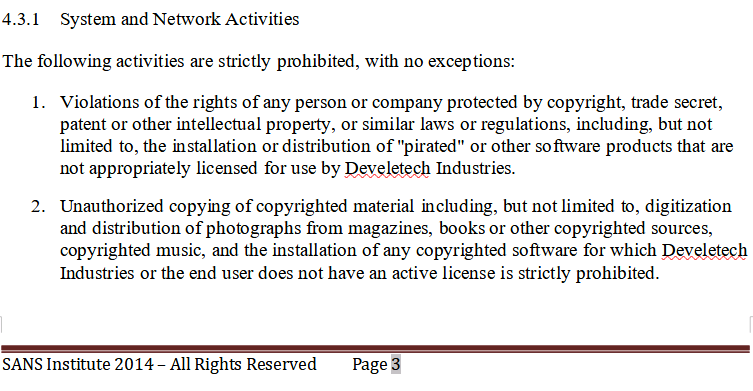
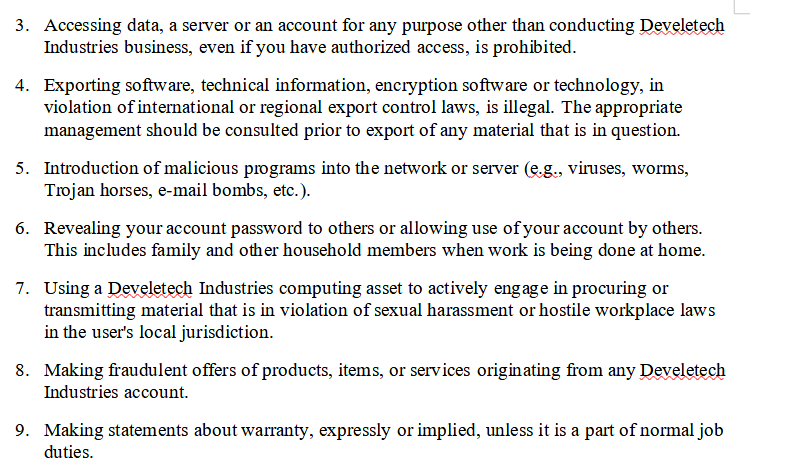
Assessing Cybersecurity Risk Lab

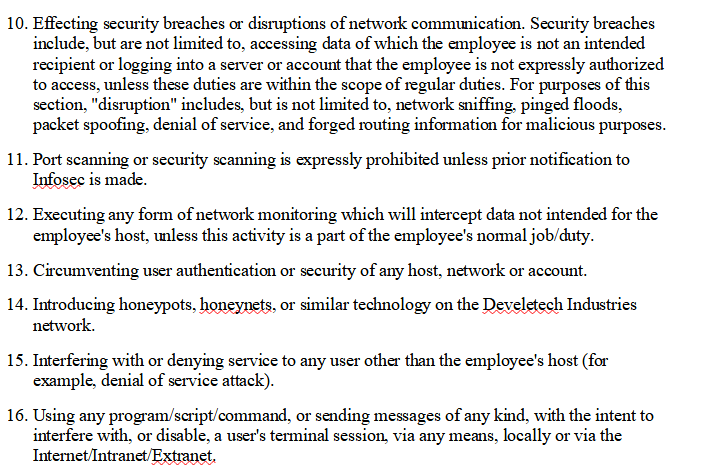
Scenario:

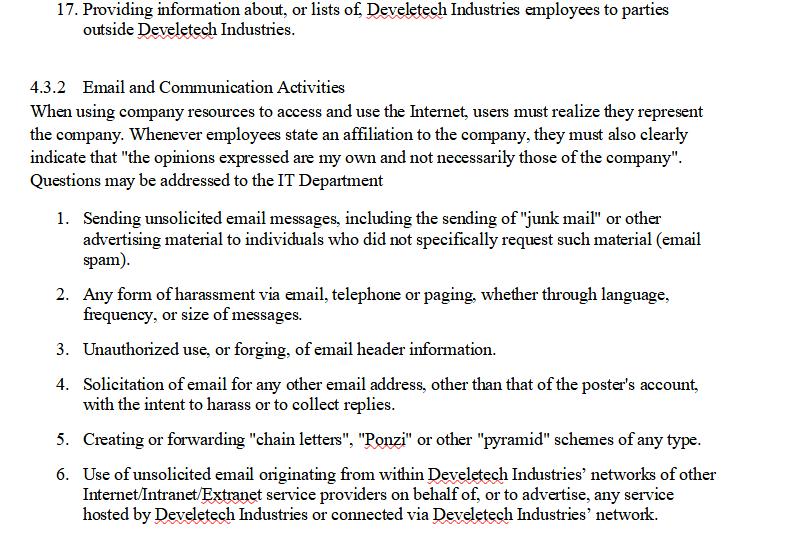
* On more than one occasion, unknown and unauthorized users have tricked Develetech's help desk employees into divulging sensitive information and exposing their workstations and the network to malicious activity. For example, users have been sending the help desk emails through personal social media services enticing the employees to click on links to malicious websites resulting in successful phishing attacks.
* **Delivery**: Employees workstation system/computer is now running sluggish or unresponsive after clicking on suspicious links. Also, attackers were successful in contacting company help desk where the help desk employees failed victim to phishing scheme resulting in company sensitive company information being exfiltrated.
* **Plan of Action:** I have decided to review Develetech's acceptable use policy so that both help desk and all other non-technical staff to be informed on what kind of behavior is or is not allowed regarding communications through non-compliance applications and services. Instead of starting from scratch, I’ll make minor adjustments to Develetech’s existing policy ensuring that the policies and procedures are up-to-date to compliance standards.
* Below is a snippet of Develetech’s unacceptable use policy to be reviewed. After reviewing their current policy, I noticed there was nothing stating how to handle communication through unauthorized channels or how to Detect and handle phishing attacks

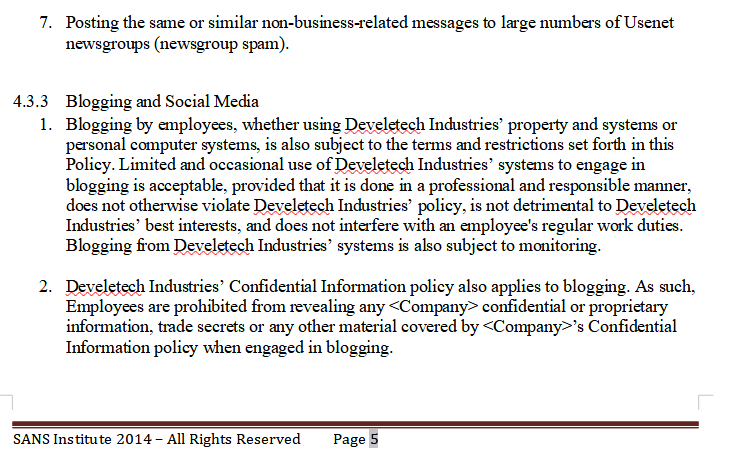


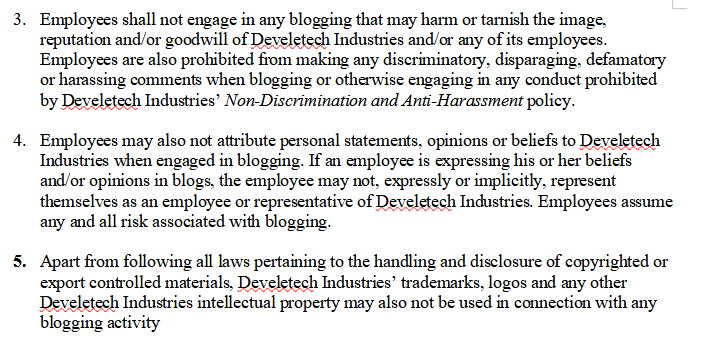












* **Remediation**: Inserted two Bullets into Daveletech AUP.
  + 8. Use of Unauthorized communication channels to contact help desk staff including the following, but not limited to, Private Social media accounts or personal email is forbidden.
  + 9. How to Detect and Handle Phishing Emails/ Solicited Messages:
    - Messages should never be sent from a public email address. Can be verified from hovering over the Email address in the from section or click on the little dropped down beside your name in the “TO” line
    - The domain name should match the user from the company reaching out without any misspellings
    - Read over the email to check to see if the message is poorly written such as grammar and syntax mistakes etc.
    - Never click on any URL links or photos without ensuring the destination is legit. Can be verified by hovering over the link. If the link is shortened via TinyUrl links do not open. If you suspect any malicious activity contact your security team immediately
    - Verify the urgency of the message before reacting such as if the email claims to be from your manager reach out to your manager through a reliable and trusted method to ensure it was in fact from them.
  + Lastly, I update the revision number and summary of change.
* Resources:
  + CertNexus for the hands-on lab [Login - OneLearn Training Management System - Skillable (learnondemand.net)](https://certnexus.learnondemand.net/User/Login)
  + Security Policy Templates which was used in this document can be found here: <https://www.sans.org/information-security-policy/>