NH Computer and Information Sciences, General. 

CIP#: 11.0101

# Cybersecurity

* Detect, prevent and mitigate threats in order to secure a computing system or network in an ethical manner, and in accordance with international, federal, state, local and cyber laws and regulations.

| **Skill/Knowledge** | **Applying**  **(4)** | **Proficient**  **(3)** | **Developing**  **(2)** | **Emerging**  **(1)** |
| --- | --- | --- | --- | --- |
| **Core Concepts**  I can effectively identify and protect Personally Identifiable Information (PII) to ensure privacy and security. |  | * I can recognize what constitutes Personally Identifiable Information (PII) in various contexts. * I can implement measures to securely handle and store PII. * I can educate others on the importance of safeguarding PII and the potential risks associated with its exposure. |  |  |
| **Hygiene**  I can demonstrate good cyber hygiene practices to maintain security and integrity on digital systems. |  | * I can manage location services settings to protect privacy and enhance security. * I can critically assess and evaluate agreements and terms of service to make informed decisions. * I can adhere to ethical principles in my digital interactions and decision-making. * I can create and maintain strong passwords to secure access to digital accounts. * I can explain the functionality of email systems, including protocols and client-server interactions. |  |  |
| **Encryption / Decryption**  I can utilize encryption and decryption techniques to ensure secure communication and data protection, including HTTPS usage. |  | * I can understand and implement encryption protocols like HTTPS to secure data transmission over the internet. * I can recognize the importance of encryption in protecting sensitive information from unauthorized access. * I can evaluate the security of websites based on their use of HTTPS and other encryption standards. |  |  |
| **Dark Web**  I can describe the concept of the dark web and its implications for cybersecurity and criminal activities. |  | * I can explain the structure and function of the dark web in contrast to the surface web and deep web. * I can discuss the potential risks and dangers associated with accessing and interacting with the dark web. * I can identify measures to protect against threats originating from the dark web. |  |  |
| **Hacking (Black vs. White)**  I can differentiate between black hat and white hat hacking techniques and understand common cyber threats such as phishing, malware, and viruses. |  | * I can distinguish between ethical hacking practices (white hat) and malicious hacking activities (black hat). * I can recognize and mitigate phishing attacks and other social engineering tactics used by cybercriminals. * I can identify different types of malware and viruses and employ appropriate measures to prevent infection and mitigate their impact. |  |  |
| **Laws & Regulations**  I can navigate relevant laws and regulations, such as copyright laws, to ensure compliance and ethical conduct in digital environments. |  | * I can understand the principles of copyright law and how they apply to digital content creation and distribution. * I can distinguish between fair use and copyright infringement in the context of digital media. * I can comply with copyright regulations when using and sharing digital content. |  |  |