IT SKILL STANDARDS 2020 AND BEYOND

“Cybersecurity”

Skillset

Acknowledgements

The development and publication of these skill standards has been a joint and collaborative effort between business and industry representatives and the education community. We are grateful to the industry personnel who participated in the development and validation process. Industry subject matter experts, technical executives, supervisors and technicians donated their time and effort to assure the relevancy of the standards 12 to 36 months into the future.

We gratefully acknowledge funding from the National Science Foundation and the leadership by the team on the IT Skill Standards 2020 and Beyond grant, based at Collin College.

Our leaders are strategically divided into Central, Western, and Eastern teams.

Central

Dr. Ann Beheler, Principal Investigator

Christina Titus, Program Director

Deborah Roberts, Co-Principal Investigator

Helen Sullivan, Senior Staff

West Coast

Terryll Bailey, Co-Principal Investigator

Dr. Suzanne Ames, Co-Principal Investigator

East Coast

Peter Maritato, Co-Principal Investigator

Gordon Snyder, Senior Staff

This material is based upon work supported by the National Science Foundation under Grant No. 1838535. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

itskillstandards.org

Cybersecurity

Approximately 100 Thought Leaders (mostly Chief Technology Officers and Chief Information Officers) agreed that this Cybersecurity Skillset would deliver “awareness plus a little more.”

This packet includes **knowledge areas as developed by subject matter experts (SMEs) via multiple synchronous meetings (see next page).**

These were developed with a focus 12 to 36 months in the future for an entry-level employee working in that specific cluster.

“Knowledge” focuses on the understanding of concepts. It is theoretical. An individual may have an understanding of a topic or tool or some textbook knowledge of it but have no experience applying it. For example, someone might have read hundreds of articles on health and nutrition, many of them in scientific journals, but that doesn't make that person qualified to dispense advice on nutrition.

The average was calculated from the subject matter expert votes.

- A vote of "4" indicated the item must be covered in the curriculum.
- A vote of "3" indicated the item should be covered in the curriculum.
- A vote of "2" indicated that it would be nice for the item to be covered in the curriculum.
- A vote of "1" indicated the item should not be covered in the curriculum.

Cybersecurity Skillset		
		Avg
K-1	Explain why knowledge of cybersecurity is important for all workers.	3.9
K-2	Explain why a computing device such as a laptop, phone, tablet, etc., should never be left such that it can provide unsecured access to sensitive data, regardless of location.	3.0
K-3	Explain why you should not leave your laptop at your desk overnight without a physical lock and a digital lock.	3.4
K-4	Explain why you should not "hold the door" for someone behind you entering an office.	3.4
K-5	Explain why you should not lend your company ID badge to someone else.	3.8
K-6	Explain how you should secure your laptop when you work from home.	3.3
K-7	Explain why you should be aware of your surroundings when having conversations or virtual meetings to ensure others can't eavesdrop on the conversations and see or hear confidential information.	3.4
K-8	Explain why you need a complex password and several guidelines for strong passwords.	3.6
K-9	Explain what multi-factor authentication is and why you should use it.	3.7
K-10	Explain why you should have a passcode or biometric verification set on your mobile phone.	3.5
K-11	Explain why you should never share your work or personal passwords.	3.8
K-12	Explain why you should not allow your children or others to use your work computer.	3.6
K-13	Explain what a VPN is and why you need to use it if you are not at the office.	3.5
K-14	Explain the risk of why you should never connect your work computing device such as a laptop, phone, bluetooth, or tablet, etc., to an open WiFi network.	2.9
K-15	Explain why your home WiFi should be password protected.	3.6
K-16	Explain why you should lock your screen when you leave your desk.	3.8
K-17	Explain why your work computer's hard drive is encrypted.	3.1
K-18	Explain why your work computer may encrypt the contents of thumb drives.	2.9
K-19	Explain why your work computer might not allow you to use thumb drives.	3.5
K-20	Explain why your work computer might block certain websites, such as personal email, social media, Google, and shared network resources.	3.3
K-21	Explain the need for hardware encryption on one's home computer.	2.4
K-22	Explain how you can tell if the information you type in a browser is safe and secure.	3.8
K-23	Explain why a document could need to be password protected.	3.3
K-24	Explain why you would "sign" a document with a public key certificate.	3.5
K-25	Explain why you would encrypt a document with a public key certificate.	3.3
K-26	Explain what is meant by Personally Identifiable Information.	3.7
K-27	Explain identity theft and methods for prevention or remediation.	3.8
K-28	Explain why you shouldn't read documents with sensitive information where others can see them.	3.4
K-29	Explain why your company may want to manage all or part of your mobile phone if you use it for any company business.	3.2
K-30	Explain why is it essential for your computers (both work and home) to have virus protection running.	3.6
K-31	Explain why your computer regularly needs to install updates and why these updates must be allowed to occur.	3.7
K-32	Explain why you should only use company approved software and programs at work.	3.8
K-33	Explain why computer systems need to be regularly backed up, both those at work and those at home.	3.3
K-34	Explain what HIPAA, PCI, PII, and GDPR are and why are they important.	3.2
K-35	Explain how to identify what public information is (anything in the public domain, or materials that are published to the public to promote the organization).	3.3
K-36	Explain what confidential information is (internal intellectual property, financial information, operating procedures, customer confidential information, and the like; often requiring NDA in place).	3.6
K-37	Explain what is meant by securing personal information (e. g., personally identifiable information, salary information, legally restricted information; requiring strict need-to-know or legal approval).	3.5
K-38	Explain why you need to be careful about clicking on unknown links, media or text links in an email or on websites, as well as the types of damage that can occur if you do.	3.9
K-39	Explain various ways to recognize a fraudulent email and how to avoid damage from it.	3.9

K-40	Explain ways to detect an email that looks like it comes from someone you know and trust, but isn't actually from them.	3.8
K-41	Identify what is meant by social engineering and how it can be used to damage cybersecurity of an organization.	3.7
K-42	Explain what is meant by phishing, spear phishing, whaling, pretexting, tailgating, and baiting and how can you detect, avoid, or mitigate their effects.	3.8
K-43	Identify the impacts of the different types of malware such as Adware, Blastware, Cryptojacking, Ghostware, Exploits, Keylogger, Ransomware, Rootkits, Spyware, Trojans, Viruses, Worms and how can you detect, avoid, or mitigate their effects.	3.3
K-44	Explain ways to tell if a text message is legitimate.	3.2
K-45	Explain how text messages or instant messages from a supposedly trusted sender can be used to gather sensitive data.	3.6
K-46	Identify watering hole attacks and how to verify accuracy of different types of received data (IM, email, or other communications).	2.9
K-47	Explains methods for telling if someone else has accessed your computer.	3.1
K-48	Explain what you should do if you suspect someone else has accessed your computer.	3.5
K-49	Explain why an email program does not show images until you specifically ask to download them.	3.0
K-50	Explain what kinds of information can you give out to people you don't know.	3.3
K-51	Explain the types of information you should NEVER give out, but instead defer to your supervisor, HR, or Legal.	3.5
K-52	Explain the concept of Zero-Trust and why you need to take such precautions.	2.9
K-53	Explain how to handle the situation when someone from work calls, tells you they forgot someone's phone number, and wants you to provide the forgotten number.	3.1
K-54	Explain what you should do if someone calls or emails you, tells you a former co-worker has given you as a reference, and wants to ask you a few questions.	2.9
K-55	Explain how you can tell whether or not someone you do not know should or should not be in the office.	3.2
K-56	Explain why your company may monitor your activity on your work computer.	3.3
K-57	Identify in general how computers, firewalls, wi-fi access points, routers, and other equipment interact with one another and why a professional cybersecurity practitioner should be the one who configures key infrastructure.	3.0
K-58	Explain the need for company rules for browsing the web, emails, and mobile usage.	3.5
K-59	Explain why you need to follow company policies and the risks to you or the company if you don't follow them.	3.6
K-60	Explain the purpose of a company's information security and data management policies.	3.6
K-61	Explain the importance of a company's change management policy.	2.9
K-62	Explain why your company may not allow you to use your company computer for personal tasks.	3.4
K-63	Explain how you should treat company-confidential documents.	3.6
K-64	Explain why you would need to verify vendor or contractor computer security measures and policy.	3.3
K-65	Describe the purpose of an information security risk assessment that evaluates both internal and external cybersecurity risks.	3.1
K-66	Explain what is meant by identity in the digital world as well as the importance of protecting it.	3.5
K-67	Explain why encryption is needed and the basics of what needs to be encrypted, as well as who is responsible for encryption.	3.4
K-68	Explain why backups are important and who is typically responsible for them.	3.4
K-69	Explain the importance of erasing all data and files from any computing device prior to disposing of it.	3.4