CYBER ESSENTIALS

Your success depends on *Cyber Readiness*. Both depend on *YOU*.

ESSENTIAL ELEMENT: YOUR DATA

THE TASK : Backup your data and configurations, and keep the backups offline

Learn to protect your information as it is stored, processed, or transmitted. Identify information critical to operations stored on your network. Have plans in place to help recover and restore systems, networks, and data from known good backups.

Essential Actions

✓ *Actions for Leaders* ✓ *Discuss with IT Staff or Service Providers*

Learn what information resides on your network. Inventory critical or sensitive information. An inventory of information assets provides an understanding of what you are protecting, where that information resides, and who has access. The inventory can be tracked in a spreadsheet, updated quickly and frequently.

Resources for Taking Action

Global Cybersecurity GCA Toolkit: *this toolkit offers free tools, practical tips, and resources and guides to improve your company's cybersecurity readiness and response.*

Cyber Readiness Institute's Cloud FAQ: Improving Cybersecurity for Remote Workers: *A guide to prioritize data to keep on your network and the information you can move to the cloud.*

Center for Internet Security (CIS) Controls Implementation Groups: *helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.*

Learn what is happening on your network. Manage network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. Actively maintaining information will give you a baseline for security testing, continuous monitoring, and making security-based decisions.

Resources for Taking Action

CISA Automated Indicator Sharing: *enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed.*

NIST draft Special Publication Zero Trust Architecture: *contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.*

NIST Special Publication 800-137: *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

NIST Special Publication 800-53 Rev 5: *Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)*

Domain Name System Protection. Domain Name System (DNS) protection blocks dangerous sites and filters out unwanted content. DNS servers ensure work devices are connecting through a secure portal. This adds a layer of protection against malware, phishing, and other viruses. Filter out connections to unauthorized websites, suspicious domain names, and known malicious domain names associated with malware and phishing. Leverage DNS filtering, also known as DNS Blocking, DNS Firewall, or protective DNS, with integrated threat intelligence. A number of effective commercial solutions are available ranging from free to low cost.

Resources for Taking Action

DNS protection – GCA Quad 9: *Quad9 protects users from accessing known malicious websites, leveraging threat intelligence from multiple industry leaders.*

NIST Secure Domain Name System Deployment Guide

ESSENTIAL ELEMENT: YOUR DATA, WHAT THE BUSINESS IS BUILT ON

Learn how your data is protected. Data should be handled based on its importance to maintaining critical operations in order to understand what your business needs to operate at a basic level. For example, proprietary research, financial information, or development data need protection from exposure in order to maintain operations. Understand the means by which your data is currently protected; focus on where the protection might be insufficient. Guidance from the Cyber Essentials Toolkits, including authentication, encryption, and data protection help identify methods and resources for how to best secure your business information and devices.

Resources for Taking Action

CIS Controls Implementation Groups: *helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.*

NIST Small Business Cybersecurity Corner: *contains guidance to help protect the security of your business information and devices.*

NIST NCCOE Data Security Program: *guidance for data integrity and data confidentiality.*

Leverage malware protection capabilities. Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.

Resources for Taking Action

Global Cybersecurity GCA Toolkit: *helps prevent phishing and viruses.*

Cyber Readiness Institute's Ransomware Playbook: *helps prioritize the data that is most critical to your organization and instructs how to back it up.*

CIS Controls Implementation Groups: *helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.*

National Cyber Security Alliance Resources Library: *tips and resources to protect devices.*

Establish regular automated backups and redundancies of key systems. Employ a backup solution that automatically and continuously backs up your business-critical data and system configurations. Regular backups protect against ransomware and malware attacks. Use on-site and remote backup methods to protect vulnerable information. Prioritize backups (based off of the importance of the information) and have a schedule of what to bring back online when so that your business can still function during a cyberattack. Test your backup strategy before you need to use it to make sure you have full read-back verification, a method of preventing errors when information is relayed or repeated in a different form in order to confirm its accuracy.

Resources for Taking Action

CIS Controls Implementation Groups: *helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.*

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations

NIST Contingency Planning Guide for Federal Information Systems

Leverage protections for backups, including physical security, encryption and offline copies. Ensure the backed-up data is stored securely offsite or in the cloud and allows for at least seven days of incremental rollback. Backups should be stored in a secure location, especially if you are prone to natural disasters. Periodically test your ability to recover data from backups.. Online and cloud storage backup services can help protect against data loss and provide encryption as an added level of security. Identify key files you need access to if online backups are unavailable to access your files when you do not have an internet connection.

Resources for Taking Action

CIS Controls Implementation Groups: *helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.*

NIST National Cyber Security Center of Excellence: *a guide for managed service providers to conduct, maintain and test backup files; protecting data from ransomware and other data loss events.*