National Campaign
for
Cyber Hygiene
Count, Configure, Control, Patch, Repeat

TOOLKIT *for* CONTROL

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Introduction

In this digital age, we rely on our computers and devices for so many aspects of our lives that the need to be proactive and vigilant to protect against cyber threats has never been greater. However, in order to be as secure as possible, we need to **use good cyber hygiene** - that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices.

The Campaign, a joint effort of the Center for Internet Security (CIS) and the Governors Homeland Security Advisors Council (GHSAC), aims to create a nationwide movement toward measurable–and sustainable–improvements in cybersecurity.

The Cyber Hygiene Campaign is a multi-year effort that provides key recommendations for a low-cost program that any organization can adopt to achieve immediate and effective defenses against cyber attacks.

The Campaign has developed toolkits for each of its key recommendations to provide easily understood instruction sheets and information for entities to improve their cybersecurity posture. The toolkits are: Count, Configure, Control, Patch and Repeat. These toolkits are dynamic documents and will continue to evolve to meet the ever-changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

Join the cause and show your commitment to getting cyber healthy by signing the online pledge! Take the Cyber Hygiene Pledge: www.cisecurity.org/cyber-pledge

Special thanks to the following individuals who were instrumental in the development of the toolkits:

- Jonathan Trull, Chief Information Security Officer
  Qualys, Inc.
- Deborah A. Snyder, Acting Chief Information Security Officer
  NY State Office of Information Technology Services
- Gary Coverdale, Assistant CIO/CISO
  Information Technology Services, Napa County, California
- Members of the Cyber Hygiene Panel

Center for Internet Security

Governors Homeland Security Advisors Council

Note: The National Campaign for Cyber Hygiene does not endorse any specific product or offering.

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

Table of Contents

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

I. Plain English Guide for Control

Basic Questions to Better Cyber Security Hygiene: Control

Cyber Hygiene Priority -- CONTROL: Protecting your systems by properly managing accounts and limiting user and administrator privileges to only what they need to do their job.

1. **Why is this step important?**
   Properly controlling access to business information and systems reduces the risk of accidents, unauthorized access/use and security breaches. Failure to properly manage access can result in compromise and loss, damage or unauthorized disclosure of sensitive and private information. Special care must be taken with "privileged accounts" used by system administrators, since they have the ability to create accounts and change or by-pass security settings. Controlling access using good processes, including the use of strong passwords reduces the risk of accounts being compromised and used for unauthorized purposes.

2. **What to do?**
   - Establish
     - Plan your account and access management program - Determine roles and responsibilities for creating, managing user accounts, privileged accounts and permissions and establish appropriate policies and procedures.
   - Control access
     - Implement processes to manage identities and credentials for authorized users and devices. Limit access to information assets and associated facilities to authorized users, processes or devices, for authorized purposes only. Use strong passwords or passphrases to help avoid user accounts being compromised. Closely manage remote access and physical access to assets.
   - Train
     - Ensure that users know how to develop strong passwords.
   - Educate
     - Make sure all users know that protecting their account credentials is their responsibility. Misuse could be attributed to them based on their unique user account.
   - Monitor
     - Log all access activities and continuously monitor to detect anomalous behavior such as unauthorized access attempts. Review access permissions, particularly privileged accounts and remote access on a regular cycle (i.e., quarterly) to confirm it is needed.

3. **Who should be responsible to do this?**
   Typically, the CIO or equivalent head of IT will be primarily responsible for designing and implementing an access management program. In addition to the CIO, the CEO, and/or the business owners of each information asset, human resources, and IT security staff should participate in developing procedures governing, granting and managing access to information assets – the business ultimately must have control over assuring only authorized users have access for authorized purposes.

4. **When to do it?**
   Access management is foundational to protecting information assets. It is a continuous process that provides the capability of protecting the confidentiality and integrity of critical data and systems by managing and securing user accounts and access. It helps ensure users only have access to what they have a valid business need for, that passwords are secure and consistently applied to all systems and applications according to security policy, and user activities are monitored and audited to ensure access is not abused.

5. **Where to start?**
   Start with user identification procedures. Work with your Human Resources Department to ensure proper employee identity verification procedures are in place for your organization. Depending on business requirements, procedures may need to include checking forms of identification against authoritative sources, background checks and screening, fingerprinting and security clearances. As an example, if you maintain confidential or sensitive records as part of your business, it would be advisable that you develop and implement procedures that meet industry compliance requirements related to access to these records. This may also require specific training steps to assure users are aware of their responsibilities related to protecting their user credentials, and accessing sensitive and confidential information.

6. **How to do it?**
   Building the governance and policy foundation to Access Control
   - Review any existing processes in place for granting/removing and managing access to assets and facilities. Confirm that processes align with desired policy, and limit access to authorized users, processes or devices, for authorized activities and transactions. Focus first on access to sensitive and confidential information. Remove unnecessary access to reduce risk wherever possible.
   - Establish a sound policy and procedure for authorizing access. Determine roles and responsibilities for vetting user identity, creating, managing user accounts, privileged accounts and permissions and granting physical access. Ensure procedures include steps for monitoring changes, audit log review and investigations and quickly suspending or retracting access if necessary.
   - Ensure user access rights align with that user's job duties. Incorporate the principles of least privilege (user has access to only what is essential to do that user's job) and separation of duties in setting up accounts and managing permissions.
   - Make sure all remote access is carefully managed. Implement processes for granting, removing and reviewing users with privileged accounts and remote access on a regular cycle (i.e., quarterly) to confirm access is still required. Consider implementing two-factor authentication for remote access (examples include password along with tokens or biometrics).
   - Communicate policies and expectations across the organization, and ensure users are educated, and understand their responsibilities for protecting user credentials and properly accessing and using information assets.

- Educate users to make sure they understand the organization's policies, and know that protecting their account credentials is their responsibility.

Implement and enforce the principle of least privilege

- Limit access to your information assets and associated facilities to authorized users, processes or devices, for authorized activities and transactions only. Manage identities and credentials for authorized users and devices. Manage physical access to assets (such as implementing a badge or key system for access to a server room)
- Implement an access control system to uniquely identify and authenticate users and devices. Require strong passwords or passphrases by system policy to reduce the risk of account compromise.
  - The stronger your passwords are, the more protected data, accounts and computing assets will be from malicious software and hackers. Two-factor authentication (token, biometrics, etc.) is recommended for remote access, particularly where access to sensitive or confidential information is concerned.
- For new IT systems and/or assets, ensure that IT staff have implemented appropriate levels of access control to properly control and monitor access to the asset before the system is moved into production. This includes removing any default or test credentials on any system before it goes live. Make sure change management procedures are in place to enable the organization to review any changes to access control procedures or system controls.
- For existing systems developed or procured prior to the implementation of an access management program, review to determine if proper access controls are in place. Develop a remediation plan to address any that are not, focusing on those that enable access to sensitive and confidential information.

Log and monitor the access control systems

- Log and monitor all access management system activities to preserve a record of when account and access privileges were granted and changed.
- Implement tools and policies that monitor and alert administrators of anomalous behavior such as unauthorized access attempts (this could include logging user access to data and/or physical assets).
  - This can be accomplished by collecting and centrally storing audit logs, and deploying a security event and incident management tool to analyze access logs against organizational policies, and report violations and anomalies. Review all noted discrepancies to determine if unauthorized access or use occurred. Ensure confirmed violations are reported to the business information owners for appropriate actions.

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

II. Technical How-To Guide for Control

Basic technical steps to better Cyber Hygiene: Control

Technical Tasks to consider

Tasks Included in level	LOE (Level of Effort - resources, effort cost) High, Med, Low	Priority How important is it for implementation of security program/controls (High, Med, Low)	Completion Criteria
Establish a plan, policies and procedures for managing identities and credentials for authorized devices and users	High	High	Plan, policy and procedures in place for authorizing access. Access control system is in place to uniquely identify and authenticate authorized users and devices.
Manage and protect physical access to assets Identify Public zones and delineate them from Work zones through the use of security controls (doors, badge control, guards, etc.)	Med	High	Policy and procedures in place for authorizing and controlling physical access (monitoring, visitor access, etc.)
Manage remote access Identify where remote access from external to your network is enabled. Establish criteria for allowing users to use remote access	Med	High	Policy and procedures in place for granting, managing and routinely reviewing remote access. Multifactor authentication; encrypted virtual private networks (VPNs), used to mitigate risk.

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Tasks Included in level	LOE (Level of Effort - resources, effort cost) High, Med, Low	Priority How important is it for implementation of security program/controls (High, Med, Low)	Completion Criteria
Set up logging for remote access authentication			
Apply the principles of least privilege and separation of duties to access permissions Identify the roles/groups of personnel working in your organization and limit their access according to the information/assets they need to access	Med	High	User access rights align with job duties (least privilege, separation of duties). Access permissions are reviewed annually, and upon significant changes in job duties. Administrative accounts are restricted, routinely monitored and reviewed on a frequent basis (i.e., quarterly).
Implement password policy and provide training for end users on how to create strong passwords	Med	High	Passwords are minimum of 8-12 characters; use UPPER and lower case characters & changed every 45 days. Different passwords are used for different accounts. Password strength testing is conducted
Require stronger authentication for access to sensitive and restricted data and systems	High	High	Multifactor authentication implemented.
Inform and Train all users on their role and responsibilities regarding account access and use.	Low	Med	Policies and responsibilities for proper access and use are reflected in awareness training and enforced.

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Resources:

For ideas on managing access and passwords, see the following links:

Resources	Link
Council on Cyber Security Critical Security Controls for Effective Cyber Defense [CSC-12, 15 & 16]	http://www.sans.org/critical-security-controls
National Institute of Standards and Technology (NIST) Special Publication 800-53 [Control Families: Access Control, Identification and Authentication, Physical Access]	http://csrc.nist.gov/publications/PubsSPs.html
Policy examples - - New York State ITS Policy P03-002, Information Security Policy, 4.1- Account Management and Access Control, and related standard. - Commonwealth of Massachusetts Enterprise Access Control Policy	http://www.its.ny.gov/tables/technologypolicyindex.htm/security http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-security-policies-and-standards/enterprise-access-control-policy.html
SANS Securing the Human end-user training	http://www.securingthehuman.org/enduser
SANS Developer and Engineer Training	http://www.securingthehuman.org/developer/demo-training-lab http://www.securingthehuman.org/engineer/ics-cyber-awareness
NIST Access Control Policy Testing Tool (ACPT)	http://www.nist.gov/itl/csd/ssa/acpt.cfm *– this is under development; check the link regularly*
National Cyber Security Alliance StaySafeOnline.org	http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securing-your-accounts
Microsoft Strong Password Tips and Password Strength Checker	http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx
Federal Communications Commission (FCC) - Cybersecurity Tips for Small Businesses	http://www.consumer.ftc.gov/articles/0009-computer-security#passwords http://www.fcc.gov/cyberforsmallbiz

Note: The National Campaign for Cyber Hygiene does not endorse any specific product or offering.

Resources	Link
National Institute of Standards and Technology (NIST) Special Publication 800-118 (Draft), Guide to Enterprise Password Management.	http://csrc.nist.gov/publications/PubsSPs.html
SANS Institute Security Policy Sample – Password Policy.	http://www.sans.org/resources/policies/Password Policy.pdf
Policy examples - - New York State ITS Policy P03-002, Information Security Policy, 4.1- Account Management and Access Control, and related standard. NYS Identity Assurance Policy and Standard.	http://www.its.ny.gov/tables/technologypolicyindex.htm/security

III. How-to measure Guide for Control

Basic ways for good Cyber Hygiene to measure progress with Control

Metrics related to controlling and monitoring accounts help reduce and manage the number of accounts. This prevents the use of compromised accounts being misused.

Useful basic metrics related to Access Control include:

- Total number of accounts with access to a given asset
- Number of accounts where the user has never logged in - unused or "orphaned" accounts are an open invitation for unauthorized access and should be suspended/deactivated.
- Number of accounts not logged in last 30 days/60 days – timeframes can be adjusted based on business needs, and used as a threshold for suspending/deactivating unused or "orphaned" accounts.
- Number of Administrator accounts
- Number of service accounts
- Number of password reset attempts – this can be used to enforce access management policies to lock the account.
- Number of policy violations identified/reported/investigated
- Number of users with remote access – it may also be helpful to track remote access activity – if it is not used for a period of time, review to see if it is really necessary.

This data will help you identify concerns and make informed access management decisions for your organization.

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

IV. Additional Resources for Control

Additional Resources to use for basic cyber hygiene in Control

Include: Links to resources (templates, etc.), automated tools that are free or low cost (such as nmap), Training options for the tools or content area (online tutorials, etc.), mentoring options (this needs to be developed)

Case Studies	**Link**
NIST Role Based Access Control	http://csrc.nist.gov/groups/SNS/rbac/case_studies.html
Physical Security	http://www.cisco.com/web/about/ciscoitatwork/case_studies/security_dl5.html
Password Management systems case studies were numerous; but all were vendor/product-specific. Do we want to include any such references? Does anyone have any others?	

The Cyber Hygiene Toolkits are dynamic documents and will continue to evolve to meet the changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

If you have expertise, resources or information relating to any of the following areas that you could share for subsequent editions of the toolkits, **please contact us at 518.880.0699 or contact@cisecurity.org**:

- Case Studies
- Webcasts, Podcasts, Videos [e.g., YouTube]
- Mentor Programs [to pair experienced individuals with those looking to gain more expertise]
- Upcoming Events [trainings, conferences, roundtable discussions]
- Other

youtube channel	**Link**
Podcasts	
CISSP Online Training. Domain: Access Control	https://www.youtube.com/watch?v=9jie8Z5hbX0
Password Management for Beginners	https://www.youtube.com/watch?v=pWYCJBBnNu0

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

V. Mapping to NIST Cybersecurity Framework for Control

How do these steps for good basic cyber hygiene in "Control" align with the NIST Framework?

"Control" maps to the following NIST Framework function(s) and Subcategories:

NIST Framework Function	Subcategory(s) / Description(s)
PROTECT (PR)	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
PROTECT (PR)	**PR.AC-2:** Physical access to assets is managed and protected
PROTECT (PR)	**PR.AC-3:** Remote access is managed
PROTECT (PR)	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties
PROTECT (PR)	**PR.AT-1:** All users are informed and trained
PROTECT (PR)	**PR.AT-2:** Privileged users understand roles & responsibilities
PROTECT (PR)	**PR.PT-1:** Audit/logs records are determined, documented, implemented and reviewed in accordance with policy.
PROTECT (PR)	**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality.
DETECT (DE)	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
DETECT (DE)	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
DETECT (DE)	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events
DETECT (DE)	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed