INTERNATIONAL COLLEGE
OF BROADCASTING

International College of Broadcasting (ICB) Information Security Policy

Revised March 2024

Contents

Policy Statement

The purpose of this policy is to provide a security framework that will ensure the protection of ICB institutional information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. ICB information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone, or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately.

Failure to comply with this policy may subject you to disciplinary action and to potential penalties described in the handbook.

As referenced by the FSA Electronic Announcement regarding updates to the GLBA cybersecurity requirements. ICB has instituted the nine elements of requirements to achieve the GLBA objective. ICB partners with NetX IT Solutions to maintain our information security program. NetX IT Solutions compiles administrative, technical, and physical safeguards that are applicable to the size and complexity of our infrastructure and sensitivity of any student's information. Within this policy we have outlined seven of the nine elements (seven applied to the size and regularity of ICB) required by FTC's regulations.[1]

Requirements in the GLBA Safeguards Rule

Element one: Designates a qualified individual responsible for overseeing and implementing the institutions or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a)).

- ICB works with NetX IT Solutions to be responsible for the oversight and implementation of all ICB's cybersecurity needs. Within this policy it, it outlines the scope and measure of NetX's responsibilities. If later information changes, ICB will work with NetX IT Solutions to institute an updated policy as well as process. ICB has designated the Campus Director ro work with NetX IT Solutions for direction and oversight with IT processes.

Element two: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student's information that could result in the unauthorized disclosure, misuse,

[1] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4

alteration, destruction, or other compromise of such information, and assesses the sufficient of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).

- Please see **page 26** of this policy that discusses ICB's Risk Assessment Policy with NetX IT Solutions.

Element three: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment. At a minimum, the right information security program must address the implement of the minimum safeguards identified in 16 C.F.R. 314.4©(1) through(8).

- ICB works with NetX IT Solutions to provide the following requirements:
  - (1) Implementing and periodically reviewing access controls, including technical and as appropriate, physical controls to:
    - (i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and
    - (ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information.
      - ICB works internally with authorized users to implement and ensure that the proper users have the proper credentials to access only applicable information. Such as, instructors do not have the same access to Financial Aid office data.
  - (2) Identify and manage the data, personnel, devices, systems, and facilities that enables ICB to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.
    - ICB ensures that the data that is stored in our third-party Student Information is not accessible to any other software system and within that system, only specified users can access information that is relevant to their role.
  - (3) Protect by encryption all information held or transmitted by both in transit over external networks and at rest. To the extent that determines encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by NetX IT Solutions.

    - ICB uses WinZip to transmit encrypted data to only government officials. However, all data that is transmitted to other entities is not sent over external networks.
- (4) Adopt secure development practices for in-house developed applications utilized by ICB for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.
    - NetX IT Solutions completes ethical hacking to determine how deep their Infosec security team can penetrate our data. The ethical hacking information is given to ICB in our monthly risk assessments to determine shortfalls or areas of opportunity to enhance our IT security infrastructure.
- (5) Implement multi-factor authentication for any individual accessing any information system.
    - Documented in this policy.
- (6)
    - (i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and
    - (ii) Periodically review your data retention policy to minimize the unnecessary retention of data.
        - Following other guidelines, ICB is required to retain data longer than two years as stated in the regulations. The data that is retained is stored in a cloud based third party Student Information System.
- (7) Adopt procedures for change management; and
    - ICB works with NetX IT Solutions to set up and regulate the user permission levels whenever onboarding or offboarding an employee. On the day of termination from employment sensitive information that was accessible in their user roles is revoked.

- (8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.
    - The process for delegating control is done by the Campus Director and NetX IT Solutions. Within the risk assessment meetings determination of activity of authorized users and unauthorized access is reviewed and if action is needed, it is rectified that day.

Element four: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

- Please see the Risk Assessment Policy located at the end of the policy.

Element five: Provides for the implementation of policies and procedures to ensure that personnel can enact the information security program.

- NetX IT Solutions performs monthly training sessions to all the employees at ICB to ensure that the employees understand the security risks associated with student information as well as network hacking. Once employees complete the training, they are given a certificate for completion that is placed in the employee file. ICB requires that service providers maintain knowledge about current threats. We verify this by requesting that the service provider attests to this.

Element six: Addresses how the institution or servicer will oversee its information system service providers.

- ICB and NetX Solutions review the information ICB’s third-party service providers have regarding safeguarding student information. If the third party does not have the appropriate security for safeguarding information, NetX provides another layer of security to prevent unethical hacking or breach of confidentiality. ICB requires that any service provider signs a contract stating that they adhere to the NIST 800-171 controls for Cybersecurity. Proof of this is required of the service provider by providing a Cybersecurity Audit report dated within 12 months or by performing a new Cybersecurity Audit and producing the report from the new audit.

Element seven: Provides for the evaluation and adjustment of its institution security program in light of the results of the required testing and monitoring, any material changes to its operations or business arrangements, the results of the required risk assessments; or any other circumstances that it knows or has reason to know may impact the material information security program.

- ICB and NetX IT Solutions review the risks of information security monthly. Upon review of whether there is a serious risk, NetX IT Solutions ensures if there is a risk that changes are made immediately, and the IT policy is updated to reflect necessary applicable changes.

Who Is Affected by This Policy

The Information Security Policy applies to all ICB faculty and staff, as well as to students acting on behalf of the International College of Broadcasting through service on ICB bodies such as task forces, councils, and committees (for example, the faculty-Student Committee on Discipline). This policy also applies to all other individuals and entities granted use of ICB Information, including, but not limited to, contractors, temporary employees, and volunteers.

Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

ICB Information – information that the International College of Broadcasting collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Policy

ICB appropriately secures its information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture.

A. Classification Levels

All ICB Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

Additional requirements for the protection of information in each classification level are identified in the ICB Information Protection Standards and Procedures.

The classifications levels are:

1. Restricted

The following ICB Information is classified as Restricted:

- Social security number
- Bank account number.
- Driver's license number
- State identity card number.
- Credit card number.
- Protected health information (as defined by HIPAA)

State and Federal laws require that unauthorized access to certain Restricted information must be reported to the appropriate agency or agencies. All reporting of this nature to external parties must be done by or in consultation with the ICB Office.

Sharing of Restricted information within the institution may be permissible if necessary to meet the institutions legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside ICB, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted information; (ii) not to disclose the Restricted information to any other party for any purpose absent the College's prior written consent or a valid court order or subpoena; and (iii) to notify ICB in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Restricted information within the institution must comply with ICB's policies including Rights, Rules and Responsibilities and Acceptable Use Policy for ICB's Information Technology and Digital Resources.

2. Confidential

ICB Information is classified as Confidential if it falls outside the Restricted classification but is not intended to be shared freely within or outside the institution due to its sensitive nature and/or contractual or legal obligations. **Examples of Confidential Information include all non-Restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records (as defined by FERPA).**

Sharing of Confidential information may be permissible if necessary to meet ICB's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside ICB, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the information: (ii) not to disclose the information to any other party for any purpose absent the institution's prior written consent or a valid court order or subpoena; and (iii) to notify ICB in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Confidential information within ICB must comply with ICB's policies including Rights, Rules and Responsibilities and Acceptable Use Policy for International College of Broadcasting Information Technology and Digital Resources.

3. Unrestricted Within International College of Broadcasting (UWICB)

ICB Information is classified as Unrestricted Within International College of Broadcasting (UWICB) if it falls outside the Restricted and Confidential classifications but is not intended to be freely shared outside ICB. One example is the Faculty Facebook.

The presumption is that UWICB information will remain within International College of Broadcasting. However, this information may be shared outside of International College of Broadcasting if necessary to meet ICB's legitimate business needs, and the proposed recipient agrees not to re-disclose the information without ICB's consent.

4. Publicly Available

ICB Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of the International College of Broadcasting.

B. Protection, Handling, and Classification of Information

Based on its classification, ICB Information must be appropriately protected from unauthorized access, loss, and damage. Specific security requirements for each classification can be found in the International College of Broadcasting Information Protection Standards and Procedures.

Handling of ICB Information from any source other than the International College of Broadcasting may require compliance with both this policy and the requirements of the individual or entity that created, provided, or controls the information. If you have concerns about your ability to comply, consult the relevant senior executive and the Office of the General Counsel.

When deemed appropriate, the level of classification may be increased, or additional security requirements imposed beyond what is required by the Information Security Policy and ICB’s Information Protection Standards and Procedures.

If you receive Controlled Unclassified Information (CUI) or create it, contact the ICB Office (ICBO) to be sure that appropriate security controls are applied to the data. If you are not sure whether it is CUI, please contact the ICBO.

5. Responsibilities

All International College of Broadcasting faculty, staff, students (when acting on behalf of the institution through service on institutional bodies), and others granted use of ICB Information are expected to:

- Understand the information classification levels defined in the Information Security Policy.
- As appropriate, classify the information for which one is responsible accordingly.
- Access information only as needed to meet legitimate business needs.
- Not divulge, copy, release, sell, loan, alter or destroy any ICB Information without a valid business purpose and/or authorization.
- Protect the confidentiality, integrity, and availability of ICB Information in a manner consistent with the information's classification level and type.
- Handle information in accordance with ICB Information Protection Standards and Procedures and any other applicable institutional standard or policy.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access ICB Information.
- Discard media containing ICB information in a manner consistent with the information’s classification level, type, and any applicable institutional retention requirement. This includes information contained in any hard copy document (such as a memo or report) or in any electronic, magnetic, or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).

- Contact the Office prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.

Contact the appropriate ICB office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

6. Related International College of Broadcasting Policies, Procedures, Standards, and Templates

- Handbook
- Data Protection Policy
- Wireless Communication Policy
- Mobile Device Standard
- Password Protection Policy
- Proper Computer Disposal
- Social Media Guidelines
- Windows Server Configuration
- Wireless Communication Standard
- Policy Compliance
- Risk Assessment Policy

7. Policy Review

At a minimum, the Information Security Policy will be reviewed every 12 months.

8. Update Log

March 16th, 2024 – Policy revised.

March 6th, 2023 – Policy revised.

November 14, 2022 – Policy issued.

Wireless Communication Policy

Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

Purpose

The purpose of this policy is to secure and protect the information assets owned by ICB. ICB provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. ICB grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to ICB's network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to ICB's network.

Scope

All employees, contractors, consultants, temporary and other workers at ICB, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of ICB must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to ICB's network or reside on ICB's site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

Policy

General Requirements

All wireless infrastructure devices that reside at ICB's site and connect to ICB's network, or provide access to information classified as ICB's Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use ICB's approved authentication protocols and infrastructure.
- Use ICB's approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to ICB's Confidential or above, must adhere to the section above. Lab and isolated wireless devices that do not provide general network connectivity to the ICB's network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the ICB's corporate network must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to ICB's corporate network. Access to the ICB's corporate network through this device must use standard remote access authentication.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- MAC Address

Mobile Device Standard

Overview

This standard defines additional terms and procedures that are important for understanding the proper use of mobile devices.

Purpose

The purpose of this standard is to provide all users with the appropriate information to abide by the Mobile Device Policy.

Scope

This standard applies to clients, patients, staff, or individuals external to ICB who own or operate a mobile device that communicates with ICB equipment, networks, or data in any way.

Standard

The following information is based on the Mobile Device Policy, which states that ICB's sensitive data should not be stored on portable computing devices unless there is no other option. The sections below are not meant to guarantee the security of your data but provide precautionary measures that should be observed.

General Guidelines

- ICB's sensitive data must not be transmitted via wireless communication to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- Don't connect to unencrypted wireless networks.
- Don't access web applications containing sensitive information.

Laptops/tablets

- Use TrueCrypt volumes for encrypted data storage.
- Use Password protected login.
- Use approved anti-virus and anti-spyware software installed.

iPhones

- Enable Passcode Lock
- Use Applications to store files in a password protected files (e.g., Private Data, Fliq Docs or any number of paid applications)

PDAs/Other Mobile Devices

- Password locks the screen.

Definitions

ICB's Network – Means any network at ICB's facilities or any network that ICB has set up for any ICB Client, Contract or Non-Contract.

Password Protection Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of ICB's resources. All users, including contractors and vendors with access to ICB's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ICB facility, has access to the ICB's network, or stores any non-public ICB's information.

Policy

Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must not use the same password for ICB's accounts as for other non-ICB access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various ICB access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Change

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

- Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to follow the Password Construction Guidelines.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential ICB information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share ICB passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All the rules above that apply to passwords apply to passphrases.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Password Construction Guidelines

Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Simple Network Management Protocol (SNMP)

Password Protection Standard

User Education –

Educate you and your staff on what is and isn't a good password. As IT professionals, most of the time we take for granted what we know. We go on with our busy days believing others already know it and the reality is that most people really don't understand how to properly create passwords and the importance of following simple standards. Users only see the end result and that is gaining access to their accounts. You should schedule 15 minutes every quarter to send out an email, or better yet, hold a small class that covers the importance of good password creation and management.

During your talk you should teach the users how to create a strong password and why it is considered a strong password. Teach them the practice of using phrases when possible. “The yellow ball is bouncing” is a considerably stronger password and much easier to remember than a keyboard smash of characters dont45$hTnflyiw0*%.

Below are some items to point out to users about password creation:

- Please do **NOT** use your name, or pet’s names or family members.
- Please do **NOT** use your Social Security Number, Birth Date, Address, Phone Number, etc.
- Please do **NOT** use any information that would be easily associated to them.
- Please do **NOT** use any password on more than one site.
- Please use at least 12 characters for a password.
- Please use the space if allowed.
- And if possible, try and create long phrases.

Teach end-users that rather than remembering passwords for every site and or account, to use a password management service like one of the following:

- LastPass – online
- 1Password – online
- DashLane – online
- KeyPass – Local application
- PasswordSafe – Local application

In short, these are all third-party services that allow a user to save all their passwords in one location and secure them with one master password.

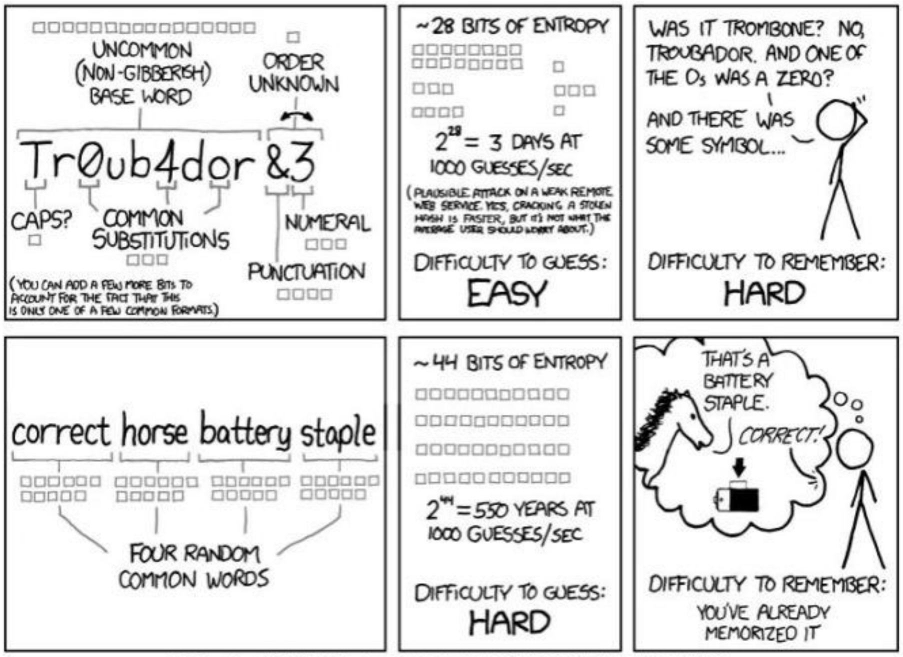
When possible, run 2FA (Two-Factor Authentication). This will greatly increase the security of the end-user account. Instruct end-users to enable and run 2FA on any of the websites that they use on a normal basis. The website https://twofactorauth.org/ is a great resource for discovering which websites currently offer 2FA.

Password Management –

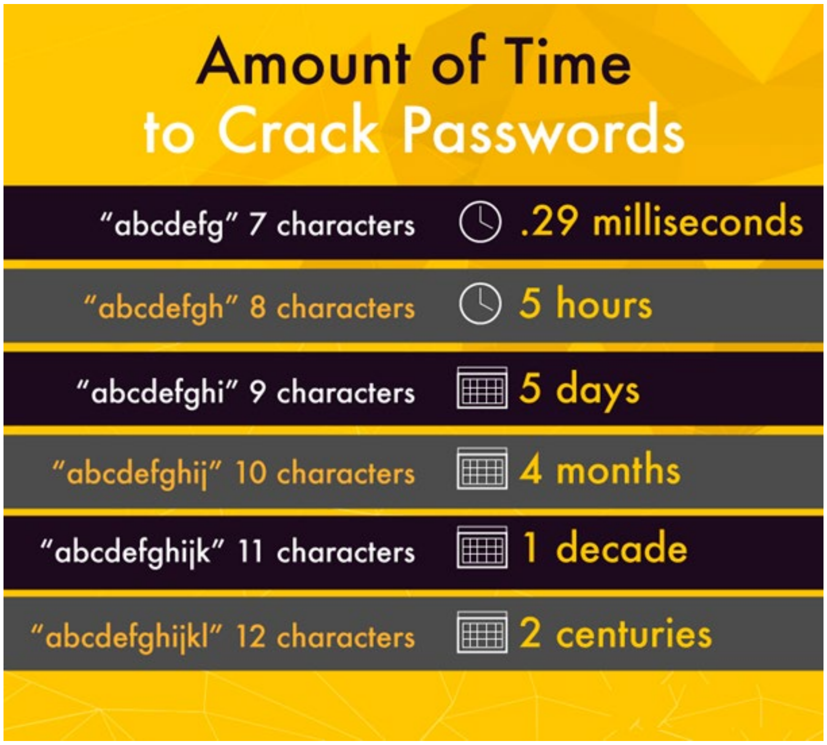
If you haven't already, now would be an appropriate time to move forward with putting in some password enforcement rules on your User Management platform (EX. Active Directory). Force users to do the following:

1. Password Length at least 12 Characters long
2. Uppercase, lowercase, numerical and character requirements.
3. Force Maximum Password Age
    - Set this to 60 or 90 days. This can be shorter if you like but, the shorter the requirement typically the weaker the passwords users create. They don't want to constantly remember and change passwords.
4. Force Minimum Password Age
    - Set this to 30 days. This will keep users from just resetting their password right back to what it was prior.
5. Enforce Password Re-use History
    - Set this to a value of 4 or higher. This will force the user to keep cycling their passwords for the entire year.

This popular xkcd comic from cartoonist Randall Munroe illustrates the efficacy of a long phrase password vs the dreaded keyboard smash.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Amount of Time to Crack Passwords

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

Proper Computer Disposal

Remove computer from Workstation location.

- Remove computer from domain when possible.
- Delete all users except Admin when possible.

Remove Hard Drive from Computer

- Mark Hard Drive with Sharpie
    - Company name
    - Status of Hard Drive
    - Date
- Place Hard Drive in Evidence bag.
- Fill out Chain of Evidence form / log.
- Place Evidence form / log in evidence bag and Seal.
- Place Evidence Bag In your locations Shred or Hard Drive Disposal Box

When Shredding or Drilling Hard Drives

- Open Evidence Bag
- Fill out and sign evidence form / log.
- Shred or Drill Hard drive.
- Place Evidence form in Destroyed Folder in office.
- Throw evidence Bag away and recycle what's left of hard drive.

Social Media Guidelines

Purpose

The purpose of this policy is to establish guidelines for staff, consultants, volunteers, members, stakeholders, and affiliated groups. This policy covers the conduct and expectations, policies, audiences, definitions, standards, guidelines & examples for employees and the public when participating in ICB's social media or social networking platforms. ICB must ensure the use of social media communications maintains our brand, identity, integrity, and reputation while minimizing legal risks, inside or outside of the workplace. Social media can move quickly and be challenging and is to be used to convey information about company products and services, promote and raise awareness of ICB brand, search for potential new markets, communicate with employees and customers to brainstorm, issue or respond to breaking news or negative publicity, and discuss corporate, business-unit and department-specific activities and events.

Definitions

<u>Social Media:</u> Social media or social networking includes all forms of online publishing and discussion, including but not limited to blogs, wikis, file-sharing, user-generated video and audio, social networks, and other social networking applications. At present, many organizations are fully engaged with social media websites such as Facebook, Twitter, YouTube, and LinkedIn, and most intend to embrace all new social media environments that may appear in the future.

Company Policy & Guidelines

Authorized users:

- Employees must be authorized by ICB's manager, based on employee job responsibilities, to engage in work-time social media sites.
- All employees must identify themselves as employees of ICB or their affiliation and expertise when posting to ICB's social media.

Content guidelines:

- For social media including ICB's, content must be relevant, meet specified goals or purposes and add value to ICB's brand.
- Any copyrighted or confidential information requires written or verbal authorization from ICB before it can be published and should be properly attributed.
- All content must conform to all appropriate laws and regulations, as well as guidelines adopted by and governing the industry, such as privacy laws.
- Content must be polite and respectful. All messaging should maintain the same tone as if interacting with someone in person on behalf of the organization.

Editorial control:

- ICB is authorized to remove any content that does not meet the rules and guidelines of the policy or may be illegal or offensive. Removal of such information will be done without permission of the author or advance warning.
- ICB expects all public users (non-employees, non-members, non-stakeholders) to abide by all guidelines of the company policy mentioned above and ICB reserves the right to take the same action as mentioned above in removing offensive or illegal content.
- Social media comments from public users that require response will be addressed in a timely but thoughtful, and respectful manner.

Personal Rules & Guidelines

Employees are expected to follow the guidelines and policies set forth below to provide a clear line between you as the individual and you as the employee of ICB.

- ICB respects the right of employees to use social media forums for self-publishing and self-expression on personal time but unless specifically authorized by department head or manager, employees are not permitted to use forms of social media during working hours or at any time on company computers or any other company-supplied devices unless the employee is authorized to speak on the organization's behalf.
- Social networking sites have blurred the line between private and public activity. In many ways, today’s social media pages have replaced the written letters of the past but are more visible. Your social media posts—even if you intend them to be solely personal messages to your friends or family—can be easily circulated beyond your intended audience. This content, therefore, represents you and the organization to the outside world.
- Employees will be held personally liable for any commentary that is considered defamatory, obscene, proprietary, or libelous by any offended party up to and including, ICB when on company’s time or using company computers or company-supplied devices.
- Employees are prohibited from harassing, discriminating, disparaging any employee or anyone affiliated with or doing business with ICB.
- Employees are prohibited from posting company’s name, trademark or logo or any company-privileged information, including but not limited to copyrighted information or company-issued documents unless authorized by ICB.
- Employees are prohibited from promoting personal projects or endorsing other brands, causes or opinions without the use of a disclaimer to separate employee’s personal uses with those of ICB.
- Employees shall use discretion in responding to public users through social media and use a respectful and courteous tone.

Enforcement

Violations of the above policy will be enforced under current employee personnel policies regarding personal conduct, supervisory discipline, reprimand, performance evaluation and/or employment termination.

Windows Server Configuration Standards

Overview

This standard defines terms and procedures for properly setting up and securing ICB's server. The configurations discussed are specific to the environment and may not work on all machines.

Purpose

The purpose of this standard is to provide all system administrators, IT staff, or other approved personnel with the appropriate information to abide by the Server Security Policy and to configure a Windows server for safe and reliable use.

Scope

This standard addresses ICB's Windows servers only.

Standard

Server Request

Prior to any server installation, the administrator must first fill out a server request form found here. Once the server has been approved, the administrator can then start the process of ordering and installing the server.

Configuration Guidelines

The following Windows specific configurations must be made.

- Install only Windows 2019 Server or newer.
- Rename the local Administrator account to something other than Administrator, and ensure it has a strong password.
- Join the local ICB domain, unless otherwise authorized by Information Systems
- Only use NTFS
- Do not use FTP, use SFTP (e.g., FreeFTPD)
- Any database server installations need to be cleared through ICB Development Support Services
- Any application that needs to run its own SMTP server, must be cleared through Information Systems
- Contact the Security Analyst for centralized logging.

Security Tools

The following tools must be installed, properly configured, and actively running on each server:

Anti-virus and anti-spyware that abides by the Anti-Virus Policy

Department Notification

Alert the appropriate departments/technicians if the server has additional needs.

- Contact the Backup Operators on what needs to be included in the backup routine.
- Contact the Network Analyst to add the server to the appropriate update reboot group in Active Directory
- Contact the Network Technician if the server needs any type of system monitoring.

Definitions

Server

For purposes of this policy, a Server is defined as an internal ICB's Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Wireless Communication Standard

Overview

See Purpose.

Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to ICB's network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to ICB's network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (Infosec) approved support organization.

Scope

All employees, contractors, consultants, temporary and other workers at ICB and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of ICB, must comply with this standard. This standard applies to wireless devices that make a connection to the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Infosec must approve exceptions to this standard in advance.

Standard

General Requirements

All wireless infrastructure devices that connect to ICB's network or provide access to ICB's Confidential, ICB's Highly Confidential, or ICB's Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from ICB's production device SSID.
- Broadcast of lab device SSID must be disabled.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to ICB's network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point.
- Disable broadcast of SSID
- Change the default SSID name.
- Change the default login and password.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

- AES
- EAP-FAST
- EAP-TLS
- PEAP
- SSID
- TKIP
- WPA-PSK

Risk Assessment Policy

Purpose

The purpose of this policy is to facilitate compliance with applicable federal and state laws and regulations, protect the confidentiality and integrity of ICB’s IT Resources, and enable informed decisions regarding Risk Management.

Scope

This IT policy, and all policies referenced, shall apply to all members of the ICB community, including faculty, students, administrative officials, and authorized guests, who use, access, or otherwise employ, locally or remotely, ICB IT Resources, whether individually controlled, shared, stand-alone, or networked.

Policy Statement

- NetX IT Solutions is authorized to perform periodic information security Risk Assessments to determine vulnerabilities and initiate appropriate remediation.

- NetX IT Solutions uses Infosec programs that identify risks and implement plans to address and manage them.
- NetX IT Solutions manages the Infosec program and coordinates the development and maintenance of program policies, procedures, standards, and reports.
- The Infosec program is based on risk assessment and developed in consideration of ICB priorities, staffing, and budget.
- Risk Assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to ICB. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing Controls to protect against these risks.
- The Risk Assessment must include the systematic approach of estimating the probability and impact of the risk and the process of analyzing the Inherent Risk score to evaluate the significance of the risk.
- Risk Assessments are performed monthly to address changes in security requirements and the risk situation (e.g., threats, vulnerabilities, impacts).
- Risk Assessments are to be undertaken systematically, capable of producing comparable and reproducible results.

Definitions

- Control - is a defined process or procedure to reduce risk.
- Inherent Risk- is the level of risk before controls are applied.
- IT Resources - include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- Risk Assessment - is the process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.
- Risk Management- is the ongoing management process of assessing risks and implementing plans to address them.

Policy Disclaimer Statement

Deviations from policies, procedures, or guidelines published and approved by NetX IT Solutions may only be done cooperatively between Infosec and the requesting entity with sufficient time to allow for appropriate risk analysis, documentation, and possible presentation to authorized ICB representatives. Failure to adhere to the written policies may be met with ICB restrictions.