CAPTRUST

Information Security Policy

2023

`

Contents

1 Overview - Executive Summary

In recognition of the critical role that information systems play in CAPTRUST business activities, this policy applies to the use of information, electronic and computing devices, and network resources to conduct CAPTRUST business or interact with internal networks and business systems, whether owned or leased by CAPTRUST, the employee, contractor, or third-party. All employees, contractors, consultants, temporary, and other workers at CAPTRUST are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CAPTRUST policies and standards, and local laws and regulation.

CAPTRUST critically depends on continued client confidence. While it is slow to grow, this confidence can be rapidly lost due to problems such as a security breach leading to system outages or data loss. The trust that clients have in CAPTRUST is a competitive advantage that must be nurtured and grown through individual efforts to comply with CAPTRUST's Information Security Policy.

The intention for publishing this policy is not to impose restrictions which are contrary to CAPTRUST's established culture of openness, trust and integrity. Information Technology is committed to protecting CAPTRUST's employees and the company from threats and illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective information security is a team effort involving the participation and support of every CAPTRUST employee, contractor, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy also defines baseline control measures that everyone at CAPTRUST is expected to be familiar with and to consistently follow. These security measures define the minimum controls necessary to prevent legal and compliance problems such as allegations of negligence, breach of fiduciary duty, or privacy violation. In some cases, these requirements will conflict with other objectives such as improved efficiency and minimized costs. Top management has examined these trade-offs and has decided that the minimum requirements defined in this document are appropriate for all employees at CAPTRUST. This document details both reasonable and practical ways for all of us at CAPTRUST to prevent unnecessary losses.

A summary of this policy is as follows:

- You are an integral part of maintaining information security for CAPTRUST.
- Information is owned by an “Information Owner” within the business who delegates safekeeping to an “Information Custodian” – typically the Information Technology (IT) Department and potentially external technology processors.
- Information is classified as Public, Internal Use (by default), or Confidential. Do not share information inappropriately – i.e., make Internal or Confidential Information Public or spread Confidential Information to a wider Internal audience.
- Access to systems is based on your job role, subject to Manager and Information Owner approval. When your employment ends, so will your access.

- Your User ID is unique to you. You are responsible for actions your User ID performs.
- Your password should be complex, difficult to guess and not the same as a password you use outside of CAPTRUST.
- For security and network maintenance purposes, IT may monitor equipment, systems and network traffic at any time. Users must have no expectation of privacy when using information systems at CAPTRUST.
- Keep your desk clean and lock away Confidential information. Do not leave PII (Personally Identifiable Information) or PHI (Protected Health Information) exposed on your desk.
- If you suspect your computer has a virus, malware or has otherwise been compromised, contact the Information Technology Helpdesk immediately.
- Monitor your printing and faxes; do not leave unattended.
- Shred anything you need to dispose of that is designated Internal Use or Confidential.
- Make sure any vendor that sees information that is designated Internal Use or Confidential has a contract in place with Non-Disclosure language. Supervise vendors very closely who do not.

  Report issues to the Information Technology Helpdesk via phone at **ext. 10500** or **(919) 576-2060** or go to **https://captrust.freshservice.com** to submit your request.

Do Not

- Use computers, email, or network to harass others, conduct illegal activities or otherwise do anything that would cast a negative light on or bring embarrassment to the Firm.
- Install software (Operating System or Applications), copy our licensed software for personal use, or attempt to hack or disrupt our network.
- Leave CAPTRUST owned mobile devices (laptops, tablets) unsecured in your office or workspace outside of business hours.
- Surf the web to sites that are inappropriate in a work environment.
- Send chain emails or forward to others. Send mass emails without engaging Marketing.
- Open suspicious emails, attachments within suspicious emails, or click on links within suspicious emails. Report such issues to IT.
- Send emails containing PII or PHI such as credit card numbers, social security numbers, dates of birth, health status, fixed passwords, or client account numbers through email or the Internet without encryption (#encrypt in subject line).
- Send or forward Firm email to a personal email (Yahoo, Gmail, etc.) or store Firm documents on a storage service like Box, DropBox, or Google Drive.
- Post information about the Firm to newsgroups, blogs, Facebook, LinkedIn, Twitter, etc., without understanding your Compliance obligations and obtaining permission, if required, from Marketing.

2 Information Security Roles & Responsibilities

2.1 ROLES

Information Security Officer —CAPTRUST's Director of Information Security serves as the Firm's Information Security Officer (ISO). He or she is expected to evaluate, report on, and suggest new ideas related to any security threats that the company currently faces, helping protect vital information and strategies.

Team Lead | Security Engineer —This role coordinates the day-to-day aspects of information security efforts, including (but not limited to), alert investigation, vulnerability remediation, incident investigation and ancillary contributions to other information security functions.

Associate II | Security Engineer —This role conducts daily reviews of current security solutions to investigate and resolve events in addition to monitoring and analyzing security alerts.

Associate | Security Engineer —This role conducts daily reviews of current security solutions to investigate and resolve events in addition to monitoring and analyzing security alerts.

Senior Team Lead | Governance, Risk & Compliance —IT Governance Risk and Compliance will coordinate and drive the day-to-day aspects of the Firm's Information Security Program as it relates to Governance, Risk, and Compliance.

Associate II | Governance, Risk & Compliance —The IT GRC Associate II will assist in executing the day-to-day aspects of the Firm's Information Security Program as it relates to Governance, Risk and Compliance.

2.2 RESPONSIBILITIES

Information Owners —Managers in user departments must be designated as the Owners of all types of information used for regular business activities. Each type of "production system information" must have an Owner. When information Owners are not clearly implied by organizational design, the Chief Technology Officer will make the designation. Information Owners do not legally own the information. They are instead members of the CAPTRUST management team who act as stewards of the information and make decisions on behalf of the organization. Information Owners or their delegates must make the following decisions and perform the following activities:

- Approve information-oriented access control privileges for specific job profiles.
- Approve information-oriented access control requests that do not fall within the scope of existing job profiles.
- Select special controls needed to protect information, such as additional input validation checks or more frequent backup procedures.
- Define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage.
- Approve all new or substantially-enhanced application systems that use their information before these systems are moved into production operational status.
- Review reports about system intrusions and other events that are relevant to their information.
- Select a sensitivity classification category relevant to their information and review this classification every five years for possible downgrading.
- Select a criticality category relevant to their information so that appropriate contingency planning can be performed.

Information Owners must designate a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time CAPTRUST employee.

Information Custodians —Custodians are in physical or logical possession of information and information systems. Like Owners, Custodians are specifically designated for different types of information. In many cases, a manager in the Information Technology department will act as the Custodian. If a Custodian is not clear, based on existing information systems operational arrangements, then the Chief Technology Officer will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners. Custodians must define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information. Custodians also define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

Information Users —Users are not specifically designated, but are broadly defined as any employee with access to internal information or internal information systems. Users are required to follow all security requirements defined by Owners, implemented by Custodians, or established by the Information Technology department. Users must familiarize themselves with, and act in accordance with, all CAPTRUST information security requirements. Users also must participate in information security training and awareness efforts. Users must request access from their immediate manager, and report all suspicious activity and security problems.

Information Technology Department—The Information Technology department is the central point of contact for all information security matters at CAPTRUST. Acting as internal technical consultants, it is this department's responsibility to create workable information security compromises that take into consideration the needs of Users, Custodians, Owners, and selected third parties. Reflecting these compromises, this department defines information security standards, procedures, policies, and other requirements applicable to the entire organization. Information Technology must handle all access control administration activities, monitor the security of CAPTRUST information systems, and provide information security training and awareness programs to CAPTRUST employees. The department is responsible for periodically providing management with reports about the current state of information security at CAPTRUST. The Information Technology department is also responsible for organizing a computer emergency response team to promptly respond to virus infections, hacker break-ins, system outages, and similar information security problems.

Information Security Audits—CAPTRUST will use internal audits and may contract with third-party firms to periodically perform audits and compliance checks to ensure that all parties are performing their assigned duties, and to ensure that other information security requirements are being consistently observed.

Information Security Alert Monitoring and Analysis—Senior Associate Security Engineer (or his Associate II) is responsible for coordination and monitoring of alerts from existing security tools, analyzing critical and high alerts as designated by CAPTRUST. Alternate staff may be assigned to support designated lead in the monitoring and analysis of relevant security alerts.

Security alerts from CAPTRUST-employed tools will be reviewed according to severity (on a daily basis).

After-Hours Security Alert Notifications—CAPTRUST receives text and email notifications on Medium and High/Critical alerts from its EDR (endpoint detection and response) system; impacted endpoints will be automatically network-isolated until further investigation and remediation can be completed. Security Engineers (Senior Associate and/or Associate II) are responsible for reviewing and responding to any such events.

Physical Security Alert Monitoring and Analysis—Senior Associate Security Engineer (or his Associate II) is responsible for coordination and monitoring of alerts from existing physical security tools. Daily physical monitoring system (Cameras and Activity) alert thresholds are set to the following:

- Changes To System(s)
- Door Held Open
- Door Forced Open
- Access Granted
- Access Denied

3 Risk Management Process

3.1 Purpose and Objectives

CAPTRUST's approach to Risk Management involves the systematic process of identifying, assessing, and responding to information security risks that could potentially impact the confidentiality, integrity & availability of client/corporate data. CAPTRUST employs multiple tools that monitor activity and alert on risks.

CAPTRUST's risk management process is defined below:

- **Risk Identification** —the process of discovering, recognizing, and documenting risk that could impact an organization.
- **Risk Assessment**—the process of identifying, evaluating and ranking risks and their potential impact to organizational assets.
- **Risk Response & Mitigation** —the process of determining the most appropriate risk-response to identified.
- **Risk & Control Monitoring & Reporting** —these functions aid the enterprise in identifying risk for assessment and mitigation.

4 Acceptable Use

4.1 General Use and Ownership

- CAPTRUST proprietary information stored on electronic and computing devices whether owned or leased by CAPTRUST, the employee or a third party, remains the sole property of CAPTRUST. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of CAPTRUST proprietary information.
- Users may access, use or share CAPTRUST proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult with the CAPTRUST Information Technology department for guidance.
- Users must not rely on the alleged identity of a correspondent through the Internet or telephone unless the identity of this person is confirmed through methods approved by the Information Technology department such as digital certificates or digital signatures.
- Users must not download software from the Internet unless specifically authorized to do so by the Information Technology department. Users may download some types of files from the Internet, but must check these files for viruses before opening or executing them. The Information Technology department maintains technology that removes unsafe attachments before they are received within CAPTRUST's systems. Depending on the file, decompression or decryption may need to be performed before downloading.
- For security and network maintenance purposes, authorized individuals within CAPTRUST may monitor equipment, systems and network traffic at any time.
- CAPTRUST reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Standard*.
- Users should apply caution when connecting CAPTRUST computers to "open" or "free" wired or Wi-Fi networks while traveling. These include, but are not limited to, airports, hotels, coffee shops and Internet cafes. Connecting to well-known providers are acceptable, examples would be Major Hotel Chains, Starbucks (Google Provided) and other Enterprise level providers. CAPTRUST-provided or personal Wi-Fi hotspots are preferred, please contact Helpdesk with questions or requests.
- System-level and user-level passwords must comply with the *Password Standard*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

- Postings by employees from a CAPTRUST email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CAPTRUST, unless posting is within the course of normal business duties.
- Employees should use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. Refer to the *Email Policy* for more detail.
- Employees should use extreme caution when clicking on hyperlinks within email messages to prevent exploitation from phishing attacks. Refer to the *Email Policy* for more detail.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of CAPTRUST authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CAPTRUST-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Questions may be addressed to the Information Technology department.

4.3.1 System and Network Activities

The following activities are strictly prohibited, without exception:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CAPTRUST.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CAPTRUST or the end user does not have an active license is strictly prohibited.
- Using CAPTRUST data or CAPTRUST owned servers for any purpose other than conducting CAPTRUST business, even if you have authorized access, is prohibited.
- Sending any sensitive Personally Identifiable Information (PII) or Protected Health Information (PHI) such as credit card numbers, social security numbers, dates of birth, health status, fixed passwords, or client account numbers through email or the Internet without encryption.
- Employees must not connect their own computers – sometimes called BYOD – with CAPTRUST computers or networks.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a CAPTRUST computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Using a CAPTRUST computing asset to actively engage in viewing, procuring, or transmitting material that is considered pornographic.
- Making fraudulent offers of products, items, or services originating from any CAPTRUST account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties or client SOW. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology department is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host (computer) unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the CAPTRUST network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet, Intranet, Extranet, unless required by client SOW.
- Providing information about, or lists of, CAPTRUST employees or clients to parties outside CAPTRUST unless this is part of employee’s normal job/duty.

4.3.2 Email and Communications Activities

- When using company resources to access and use the Internet, users must realize they represent the company. The following activities are prohibited:
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email SPAM).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Sending any sensitive parameters such as credit card numbers, social security numbers, fixed passwords, or client account numbers via email without the use of encryption.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within CAPTRUST's networks or other Internet, Intranet, Extranet service providers on behalf of, or to advertise, any service hosted by CAPTRUST or connected via CAPTRUST's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging, Posting, and Social Media

- Blogging and content posting by employees, whether using CAPTRUST’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CAPTRUST’s systems to engage in blogging and content posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CAPTRUST’s policy and compliance obligations, is not detrimental to CAPTRUST’s best interests, and does not interfere with an employee's regular work duties. Blogging and content posting from CAPTRUST’s systems is also subject to monitoring.
- CAPTRUST’s Confidential Information policy also applies to blogging and content posting. As such, Employees are prohibited from revealing any CAPTRUST confidential or proprietary information, trade secrets or any other material covered by CAPTRUST’s Confidential Information policy when engaged in blogging or content posting.
- Employees shall not engage in any blogging or content posting that may harm or tarnish the image, reputation and/or goodwill of CAPTRUST and/or any of its employees. Employees are also prohibited from making any discriminatory,

disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CAPTRUST's Human Resources policies.

- Employees may also not attribute personal statements, opinions or beliefs to CAPTRUST when engaged in blogging or content posting. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of CAPTRUST. Employees assume any and all risk associated with blogging and content posting.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, CAPTRUST's trademarks, logos and any other CAPTRUST intellectual property may also not be used in connection with any blogging or content posting activity.

5 Password Policy

5.3 Password Construction

Passwords are a critical component of information security. This guideline provides best practices for creating secure passwords. This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router and switch logins.

5.3.1 Password Construction Guidelines

All user passwords should meet or exceed the following guidelines. Strong passwords have the following characteristics:

- Contain at least 16 characters
- Contain at least one special character (!@#$%^&*()_+)
- Combination of 4 to 5 *random* words

Poor or weak passwords have the following characteristics:

- Contain 15 characters or less
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome12345678" "Password1234567" "Changeme1234567"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

5.3.2 Password Protection

All users, including contractors and vendors with access to CAPTRUST systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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 CAPTRUST facility, has access to the CAPTRUST network, or stores any non-public CAPTRUST information.

- Users must not use the same password for Windows log-in (desktop/laptop) and CAPTRUST accounts maintained in the cloud. Use the capabilities of CAPTRUST's single-sign-on solution (Okta) to remember passwords for CAPTRUST-related web sites maintained outside of CAPTRUST.
- Users must not use the same password for CAPTRUST accounts as for other non-CAPTRUST access (i.e., personal email account, social media account, etc.).
- Where possible, users must not use the same password for various CAPTRUST access needs.
- All user-level passwords will not be changed unless an area of compromise is suspected.
- Passwords must not be shared with anyone at any time. All passwords are to be treated as sensitive, confidential CAPTRUST information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone, even CAPTRUST Helpdesk personnel.
- Do not reveal a password on a questionnaire or security form.
- Do not hint at the format of a password (i.e., "my family name").
- Do not write passwords down and store them anywhere in your office or workspace. Do not store passwords in a file on a computer or mobile device without encryption.
- Do not use the "Remember Password" feature of applications (web browsers). Instead, use the capabilities of CAPTRUST's LastPass to remember passwords for web sites outside of CAPTRUST.
- Any user suspecting that their password may have been compromised in any way must report the incident and change all applicable passwords.

6 Electronic Mail Policy

The purpose of this section is to ensure the proper use of CAPTRUST email systems and make users aware of what CAPTRUST deems as acceptable and unacceptable use of its email systems. This policy outlines the minimum requirements for use of email within the CAPTRUST network. The policy covers appropriate use of any email sent from a CAPTRUST email address and applies to all employees, vendors, and agents operating on behalf of CAPTRUST.

- All use of email must be consistent with CAPTRUST policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- CAPTRUST email accounts should be used primarily for CAPTRUST business-related purposes; personal communication is permitted on a limited basis, but non-CAPTRUST related commercial uses are prohibited.
- All sensitive CAPTRUST data contained within an email message or an attachment must be secured using an approved form of email encryption.
- Electronic mail systems must not be used for message storage. All electronic mail messages which flow through CAPTRUST mail servers are archived for compliance and retention purposes. Employees have access to search their personal archive to find any message that may have been removed from their mailbox based on CAPTRUST's email retention policy.
- The CAPTRUST email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any CAPTRUST employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding CAPTRUST email to a third-party email system (noted below). Individual messages which are forwarded by the user must not contain CAPTRUST confidential information.
- Users are prohibited from using third-party email systems and storage servers such as Google / Gmail, iCloud, Yahoo, and Outlook.com / MSN Hotmail etc. to conduct CAPTRUST business, to create or memorialize any binding transactions, or to store or retain email on behalf of CAPTRUST. Such communications and transactions should be conducted through proper channels using CAPTRUST approved documentation.
- Using a reasonable amount of CAPTRUST resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a CAPTRUST email account is prohibited.
- CAPTRUST employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- CAPTRUST may monitor messages without prior notice. CAPTRUST is not obliged to monitor email messages.

7 Mobile Computing and Remote Access Policy

Remote access to our corporate network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are maintained with less rigorous security than the CAPTRUST network. While remote networks are beyond the control of the CAPTRUST policy, we must mitigate these external risks to the best of our ability.

The following applies to all CAPTRUST employees, contractors, vendors and agents with a CAPTRUST-owned or personally owned computer or workstation used to connect to the CAPTRUST network. This policy applies to remote access connections used to do work on behalf of CAPTRUST, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to CAPTRUST networks.

- Secure remote access must be strictly controlled with encryption (i.e., VPN client, Citrix, or OWA) and strong account passwords.
- Remote access to all Okta Authenticated Applications require Multi-Factor Authentication be setup. (Failure will result is remote access restriction)
- Authorized users shall protect their login and password, even from family members.
- While using a CAPTRUST owned computer to remotely connect to the CAPTRUST corporate network, authorized users shall ensure the remote computer (host) is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.
- Use of external resources to conduct CAPTRUST business must be approved in advance by Information Security and the appropriate business unit manager.
- All computers (hosts) that are used to connect to the CAPTRUST corporate network via remote access technologies must use a reliable and updated endpoint control application.

8 Clean Desk Policy

The purpose of this section is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers, and our vendors is secure in locked areas and out of site. A Clean Desk policy is part of standard basic privacy controls.

- At the end of the workday and at any time when the employee is going to be away for more than 15 minutes, employees must secure all Non-Public Information (NPI), Personally Identifiable Information (PII), and Protected Health Information (PHI) in addition to sensitive/confidential information in paper or electronic form.
- Lock computer workstations (Ctrl-Alt-Delete ⟶ Lock or the Windows key-L key combination will immediately lock any Windows workstation) when workspace is unoccupied.

- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked, or stored in a locked file room, when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords and PINs should never be written down in a notebook or Post-it Notes or left under a keyboard, or otherwise physically hidden in an office.
- Documents containing Restricted or Sensitive information should be immediately removed from copiers, unattended printers and fax machines.
- Upon disposal Restricted and/or Sensitive documents should be placed in locked shred-it disposal bins.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer when not in use.
- Electronic media (CD-ROMs, USBs, etc.) should be given to IT for proper disposal.
- Whiteboards containing Restricted and/or Sensitive information should be erased after meetings.
- Portable computing devices such as laptops and tablets should be taken home by employees. If not, they should be locked-away when leaving the office.
- Passwords and PINs should never be written down in a notebook or Post-it Notes or left under a keyboard, or otherwise physically hidden in an office.

Clean Desk Policy —Work from Home (WFH)
(includes all applicable procedures listed in the bullet points in addition to those found below)

- Employees who are required to print CAPTRUST documents at home or scan from personal devices are required to:
  - Have written approval from their manager prior to installation of necessary drivers to operate personal printing, or
  - Scanning peripherals from the employee’s CAPTRUST-issued laptop.
- Properly shred documents when no longer needed for their responsibilities (meetings/presentations/etc.) by using:
  - A cross-cut shredder (preferred) to destroy CAPTRUST documents at the home of the employee in question

Deliver documents to CAPTRUST offices, depositing documents in locked Shred-It disposal bins. If an employee chooses this method, they must keep sensitive papers secured in a reasonable manner prior to shredding.

9 Printing, Copying and Fax Transmission

Destruction of Waste Copies —If a printer, copier, or fax machine jams or malfunctions when printing Confidential information, the involved users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information must be disposed of by shredding or other methods approved by the Information Technology department.

Faxing Precautions —Sensitive materials must not be faxed unless an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, the fax is sent to a locked room to which only authorized employees have access, or a password-protected fax mailbox is used to restrict release to an authorized recipient. Sensitive information must not be faxed through untrusted intermediaries such as hotel staff or rented mailbox service staff. The receipt of sensitive information by fax must be confirmed promptly. All faxes must employ a standard cover page that includes language approved by the CAPTRUST Legal and Compliance departments. Third-party signatures on contracts, purchase orders, and similar legal documents sent by fax must always be followed-up with an exchange of paper originals.

Printer Precautions —When printing sensitive information, the user must be present at the printer at the time of printing to prevent the information from being revealed to unauthorized parties or direct the output to a printer inside an area where only authorized employees are permitted. Printed materials including sensitive information must not be left on printers, copiers or fax machines.

Copy Machine Precautions —Unless permission from the copyright Owner is obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary.

Repair Services —The repair of fax machines, printers, and copy machines must be performed only by third-party vendors who have signed a CAPTRUST non-disclosure agreement. Any permanent storage within a fax machine, printer or copier should be erased following the *Information Destruction Standard* prior to removal from CAPTRUST.

10 Information Sensitivity Classification

CAPTRUST regards all client information as confidential and protects it as such. CAPTRUST also regards all other information contained within its networks as confidential unless otherwise approved by Compliance and Marketing.

11 Access Control

Access Philosophy —Access to Public and Internal Use information is not restricted with access controls that discriminate by specific user. For example, Public information is available on the CAPTRUST web site, and Internal Use information is available on the CAPTRUST intranet. Access to Confidential information must be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information Owner. Access to special hardware and software must be restricted based on business need.

Access Approval Process —An employee's manager must initiate the access control approval process, and the privileges granted remain in effect until the employee's job changes or the employee leaves CAPTRUST. If either of these two events occur, the Human Resources department must notify the Information Technology department immediately. All non-employees, contractors, consultants, temporary employees, and outsourcing organizations must also go through a similar access control request and authorization process initiated by the project manager. The privileges of these non-employees must be immediately revoked by the Information Technology department when the project is complete, or when the non-employees stop working with CAPTRUST. The relevant project manager must review the need for the continuing privileges of non-employees every three months.

Departures from CAPTRUST —When a user leaves CAPTRUST, all system privileges and access to CAPTRUST information must cease immediately. For example, departed users must not be permitted to continue to maintain an electronic mail account with CAPTRUST. At this point, all CAPTRUST information disclosed to users must be returned or destroyed. For example, client contact lists must remain with CAPTRUST, unless otherwise approved by Senior Management. All work done by users for CAPTRUST is CAPTRUST property, and it too must remain with CAPTRUST when users depart.

Unique User IDs —Every CAPTRUST user ID and related password is intended for the exclusive use of a specific individual. User IDs are linked to specific people, and are not associated with computer terminals, departments, or job titles. Except for Internet pages, intranet pages, and other places where anonymous interaction is both generally understood and expected, anonymous and guest user IDs are not permitted unless approved in advance by the Information Technology department.

User Authentication —Users are responsible for all activity that takes place with their user ID. A user must change their password immediately if they suspect that it has been observed or discovered or used by another person. Users must notify Information Technology if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

12 Reporting Problems

What to Report —All employees must promptly report to the Information Technology department any loss of, or severe damage to, their hardware or software. Employees must report all suspected compromises to CAPTRUST information systems. All serious information security vulnerabilities known to exist must be reported. All instances of suspected disclosure of sensitive information also must be reported.

How to Report —All problems must be reported to the Information Technology helpdesk via phone at **ext. 10500** or **(919) 576-2060** or go to **https://captrust.freshservice.com** to submit your concern. Reports must not be sent by electronic mail unless the message is encrypted with software authorized by the Information Technology department. All reports must be investigated before any action is taken. Employees may also use the helpdesk line for questions about information security.

13 Policy Compliance

13.3 Compliance Measurement

Compliance to this policy will be verified through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

13.4 Exceptions

Any exceptions to this policy must be approved by the Governance, Risk, and Compliance department in advance.

13.5 Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. CAPTRUST reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

14 Policy Maintenance

This policy must be reviewed at least once per year by the Information Technology department and updated accordingly to reflect any changes in technology, process, or procedure.

15 Approval and Ownership

Created By	Title		
Nick Brezinski	Director		
Updated By	**Title**		
Jon Atchison	Senior Team Lead		
Approved By	**Title**	**Date**	**Signature**
Nick Brezinski	Director	3/13/2023	DocuSigned by: Nick Brezinski C746400D55FA4F7...
Jonathan Meyer	Chief Technology Officer	3/8/2023	DocuSigned by: Jon Meyer 7DC3E41218784A2...
Denise Buchanan	Chief Compliance Officer	3/15/2023	DocuSigned by: Denise M Buchanan 8A2795DEC786419...

16 Revision History

Version	Revision Date	Review Date	Description
1.0	7-6-2010	7-6-2010	Policy Creation
2.0	7-20-2011	7-20-2011	General Updates
3.0	5-3-2016	5-5-2016	InfoSec Updates
4.0	10-24-2017	10-26-17	InfoSec Updates
5.0	01-08-2021	01-08-2021	InfoSec Updates
5.5	10-18-2021	10-20-2021	InfoSec Updates
6.0	2/28/2023	2/28/2023	InfoSec Updates