INFORMATION SECURITY POLICY

Table of Contents

1. Introduction 2
2. Prohibited Use Policy 3
3. Malware and Antivirus Policy 4
4. Email Usage Policy 5
5. Internet Usage Policy 6
6. Password Policy 7
7. Data Backup Policy 8
8. Definitions 10
Introduction

Background
Cetera Financial Group (Cetera) shall provide employees with direction for the secure use of Cetera information and systems. The ultimate goal is the safeguard of Cetera’s information wherever it resides. Information may reside on computers, cell phones, networks, printed media, digital media, physical storage, or a person’s memory. Employees and contingent workers are obliged to adhere to these policies and shall report infractions according to established response procedures.

Policy Scope
This policy applies to all Cetera proprietary information whether it is utilized by employees or contingent workers. Employees and contingent workers are required to read and acknowledge this policy prior to being given access to any Cetera resource.

User Responsibilities
1. Cetera employees and contingent workers shall attend all required security training.

2. Cetera employees and contingent workers shall protect their system passwords at all times. These items are never to be shared with family members or friends, even when working from home.

3. Cetera employees shall abide by the controls and policies covered in the Employee Handbook.

4. Cetera employees and contingent workers shall report any violations or weaknesses of Cetera’s security policies to their supervisor.

5. Cetera employees and contingent workers shall report any information security incidents to SecIncidents@Cetera.com in a timely manner.

It is very important the incident response process starts as soon as an information security incident is identified. If you are not sure whether something qualifies as an information security incident, be safe and follow the process described below as soon as you can. The Incident Response Team will determine if it’s an information security incident for you. Examples of incidents include:

- The loss or potential loss of confidentiality of any nonpublic information (such as personally identifiable information) through the loss/theft of a laptop, PDA, Blackberry or smartphone
- Potential compromise of the integrity of any Cetera information
- Improper handling or disposal of proprietary or nonpublic data
Prohibited Use Policy

The following system and network activities are strictly prohibited except in cases where employees are exempted from these restrictions during the course of their legitimate job responsibilities (i.e., 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 Cetera authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Cetera-owned resources. The list below is not exhaustive and attempts to provide a framework for activities that fall into the category of unacceptable use.

- Exporting software, technical information, encryption software or technology that is in violation of international or regional export control laws. The appropriate management personnel should be consulted prior to export of any material that is in question.

- 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.

- Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any computer, network or account.

- Disrupting services on a computer other than your own.

- Using any program/script/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.
Malware and Antivirus Policy

Background
Viruses and other forms of malicious code (sometimes known as malware) represent a significant threat to Cetera computer resources. This policy provides structure for protecting Cetera resources from these threats by limiting exposure using industry best practices. This includes desktop antivirus programs, server antivirus programs, and controls to reduce the probability of introducing malicious software into our environment. Reducing the impact and threat of viruses and malware requires active participation by everyone. Viruses can be introduced into an environment through common user actions, like opening an attachment in an email or downloading a program via the Internet. Actively protecting a computer can make a significant difference whether a virus spreads, is quickly contained, or is never introduced.

Policy Scope
This policy applies to all employees and contingent workers who access Cetera computer networks. Throughout this policy, the word user will be used to collectively refer to all such individuals.

Standards
*Users encountering computer viruses.* If users suspect infection by a virus, they must immediately notify the Cetera Help Desk. Trying to remove a suspect infection may cause the damage to spread and impair the ability to remove the infection.

*Downloading software from suspicious or unknown sources.* Downloading, forwarding, or introducing software from suspicious, unknown, or untrustworthy sources greatly increases the risk of introducing a virus into our environment. Such software may contain viruses, worms, Trojan horses, spyware, or other software that may compromise Cetera data and systems.

*Virus scanning at servers and desktop machines.* Cetera’s antivirus software performs weekly scanning of the entire hard drive along with active scanning of any new files opened. If there are business reasons to disable the scanning to minimize conflict with other computer activities, please contact the Cetera Help Desk. Never attempt to disable the antivirus software yourself at any time without receiving approval from Cetera’s Help Desk.

*Antivirus signature updates.* Always keep the antivirus signatures up to date. Users who have not connected to Cetera’s network for an extended amount of time may not have the latest antivirus signatures. If the user believes there may be an infection during this time, do not connect the computer to Cetera’s network before contacting Cetera’s Help Desk.
Email Usage Policy

Background
This policy serves to educate on the proper usage of emails that would minimize the risks associated with being noncompliant with regulatory laws and tarnishing Cetera’s image. With the instantaneous and powerful nature of email communication, it is very important that email is used correctly. For example, Cetera’s email system does not automatically encrypt messages; therefore, confidential information should not be included in your messages unless you manually encrypt the messages. If you are unclear on the secure nature of your email, please contact Cetera’s Help Desk before sending anything confidential via your Cetera email account.

Procedure
For Cetera home office users (mailboxes that have an @cetera.com, @multifinancial.com, @financialnetwork.com, or @primevest.net address), outbound emails can be encrypted using the word “Secure:” in the subject line of the email.

Policy Scope
This policy covers the use of email sent from a Cetera email address and applies to all employees and contingent workers.

Standards
Prohibited use. The Cetera email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Anyone at Cetera who receives any emails with this content from any Cetera employee or contingent worker should report the matter to their supervisor immediately.

Personal use. Using a reasonable amount of Cetera resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work-related email. Using email for non-productive activities like gambling, sports leagues, or electronic gaming is prohibited. Virus or other malware warnings and mass mailings from Cetera shall be approved by Cetera Information Security or Cetera Marketing before sending. These restrictions also apply to the forwarding of mail received by a Cetera employee.

Monitoring. Cetera employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. Cetera may monitor messages without prior notice. All emails are archived and randomly reviewed for compliance.
Internet Usage Policy

Background
Cetera accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. The use of the Internet is permitted and encouraged where such use supports the goals and objectives of the business. The policy serves to guide employees and contingent workers on what is proper usage of the Internet. Using the Internet improperly may lead to unnecessary risk being introduced into the company.

Policy Scope
This policy covers appropriate use of Internet access from any Cetera office or with Cetera-owned equipment, by any employee or contingent worker.

Unacceptable Behavior
In particular the following is deemed unacceptable use or behavior:
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license
- Hacking into unauthorized areas
- Undertaking deliberate activities that waste staff effort or networked resources
- Knowingly introducing any form of malicious software into the corporate network

Company-Owned Information Held on Third-Party Websites
If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Cetera. This includes any such information stored on third-party websites, such as webmail service providers, and social networking sites, such as LinkedIn.

Monitoring
All of the company's Internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of Internet and network traffic, together with the Internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
Password Policy

Background
Passwords provide an effective layer of protection, but only when they are strong. The purpose of this section is to define account and password policies for Cetera systems that will minimize the chances of a user account being compromised. These standards are intended to strengthen the authentication and account management for Cetera systems and applications that receive, process, store, transmit and/or dispose of restricted and protected information.

Policy Scope
This standard defines the specific rules around user IDs and passwords for internal Cetera systems. This includes not only the production environment but also all test, development, and QA.

General User Standards
- User-level passwords are required to be strong, meaning they must contain at least eight characters, including characters from three of the following categories:
  1. Uppercase letters (A–Z)
  2. Lowercase letters (a–z)
  3. Digits (0–9)
  4. Non-alphanumeric characters such as an exclamation point (!), dollar sign ($), number sign (#), or percent sign (%).

- User-level passwords (e.g., for email, desktop, laptop, mobile device) expire every 90 days. Users are encouraged to change them more frequently if possible.

- User-level passwords kept in storage (e.g., in an Excel or text file) should be protected by reasonable means such as a strong password or encryption.

- A username and corresponding password, in plain text, must never be inserted into the same email or other form of electronic communication.
Data Backup Policy

Background
This policy states the requirements for backing up and recovering data on all systems that house unique data within Cetera’s environment. The purpose is to ensure that continuity of the availability, integrity, and confidentiality of data necessary for business operations continues in the event of personnel, hardware or software failures.

Policy Scope
This policy applies to all Cetera information systems, employees and contingent workers.

Standards

User Requirements
- All individual business documents shall be stored in the user’s My Documents folder.
- All shared business documents shall be stored in the designated shared drive (e.g., the H, I or S drive).
- Personal documents should not be stored on corporate resources and will not be backed up.

IT Backup and Recovery Policy Reference
- All Cetera backups shall be tested on a regular basis. The security of the recovered data shall be maintained at all times with the recovered data being destroyed after testing has concluded.
- Full backups will run on weekends with incremental backups running daily.
- Data containing personal identifiable information shall be encrypted.
- All Cetera backup media shall be classified as protected.
- All Cetera backup media shall be retained in accordance with any applicable laws and regulations.

Audit
Compliance with this agreement is subject to audit by the Information Security Office and internal auditors.

Review
This policy shall be reviewed on a periodic basis to ensure that it remains appropriate for the Cetera business operations.

Exceptions
There may be instances where there is a justifiable business need to perform actions that are in conflict with Cetera policies and procedures. Cetera recognizes that policies and procedures cannot be created and enforced to address all business issues. The following principles apply to exceptions:
- Requests for exceptions to policies and procedures must have a justifiable business case.

- Exceptions are valid for a maximum of one year, at which time the exception must be reevaluated and reapproved.

- If procedure exceptions will circumvent existing internal controls, then mitigating or compensating controls should be implemented. The Information Security Office, Cetera IT Operations and the Information or Process Owner must be involved in all instances where the bypassing of information security controls will result in residual risk to Cetera.
Definitions

Account  A representation of a user in a system.

Authentication  The process of identifying and verifying a user through presentation of a valid user ID and password.

Cetera Information Security  Members of Cetera Information Security are responsible for information security concerns described in the Cetera Information Security charter. The Cetera ISO advises on security controls, defines security architecture, facilitates security risk management, leads the security incident response process, and performs security assessments. Cetera Network Engineers and Cetera Security Fulfillment handle the daily operational security functions.

Cetera Information Security Office  The Information Security Office (ISO) is accountable and responsible for managing and directing the information security program.

Cetera IT Operations  The people, processes, and technology employed to ensure the health and well-being of the Cetera technical environment.

Cetera security policies  The policies established by Cetera that define the rules for addressing confidentiality, integrity, and availability for Cetera resources.

Chain email or letter  Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Computing environment  A collection of computers, telecommunications and network equipment, applications, and wiring that support the processing and communication of electronic information.

Contingent worker  Any person with whom Cetera has a direct contractual relationship, including employees or agents of third parties, vendors, dealers, affiliates, and applicable contingent workforce providers. These may also be known as contractors, vendors, consultants, and third-party resources.

Contracts and purchase orders  Legal agreements between Cetera and another entity (e.g., a corporation, partnership, or individual) describing products and/or services to be delivered.

Controlled area  Any area within Cetera where identification, authentication, and credentialing are required to gain admittance.

Credentials  The means and manner by which access is granted to a specific resource. This can include user IDs, passwords, badges, tokens, and keys.

Default password  A password that is preset on a computer system either by a manufacturer or by a system administrator.

Email  The electronic transmission of information through a mail protocol such as SMTP, POP3, or IMAP. Typical email clients include Microsoft Outlook, Entourage, Apple Mail, or Eudora.
Employee  Any Cetera or Cetera affiliate employee whether full time or part time, exempt or non-exempt, working on company premises or remotely, who is paid directly from Cetera or an affiliate and can participate in company benefits.

Encryption  The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people. Refer to the Cetera Encryption Policy for details.

Forwarded email  Email resent from the original recipient to one or more additional email recipients.

Idle session timeout  Refers to the time that the system will allow a session to be valid while being in an inactive state before the system will automatically terminate the session.

Incident  An occurrence or event that can negatively impact the safety, security, or continued operations of Cetera.

Information exchange agreement  A formal agreement between two parties that describe the conditions, means, and manner under which information may be transferred.

Media  Any physical or technical materials used to place, keep, and retrieve data or information. Examples of media include paper files, electronic files, email, tapes, CDs, DVDs, etc.

Password  A secret sequence of characters known only to the user. Passwords are used during authentication to prove the identity of a user.

Password history  Password History defines the number of unique new passwords that must be associated with a user account before a previously used password can be used.

Port scanning  The act of probing a machine for open ports for the purpose of finding active ports which can be used to exploit known weaknesses in an operating system or application.

Privileged user  Any user or account that has the ability to grant, modify, or deny other accounts access to Cetera resources.

Service account  Infrastructure system account not uniquely assigned to any information user. Examples of service accounts include but are not limited to directory access service accounts, database service accounts and root accounts.

Spam  Email sent in bulk, usually to indiscriminate recipients.

System  Any computer or device or any combination of these components taken together to form an application.

System owner(s)  The individual(s), business unit(s) or business owner(s) in the organization who is held accountable for the IT system and the data that system contains.

Third parties  Any entity that interacts with Cetera but is not directly affiliated. For example: clients, contractors, subcontractors, government agencies, vendors, unions, etc.

Trojan horse  A malicious program that masquerades as a benign application.
**Virus**  An unauthorized program that replicates itself and spreads onto various data storage media and/or across a network.

**Unauthorized access**  Access to Cetera facilities, systems, or possession of business information or data by people who are not Cetera employees, Cetera contingent workers, or authorized by Cetera Information Security.

**User**  Any person that provides, collects, handles, accesses, or processes information using a system.

**User ID**  A unique identifier and property of an account. It is associated with the user assigned to the account.
CETERA INFORMATION SECURITY POLICY AGREEMENT

ACKNOWLEDGEMENT

I acknowledge that I have received the Information Security Policy. I have read the Information Security Policy and understand that I must comply with it when accessing and using Cetera information resources. My failure to comply with the Information Security Policy Agreement may result in cancellation of my privilege of use of Cetera’s information and systems, and/or appropriate disciplinary action.

Name

Title

Date

Signature