Security Incident Response Plan

For Clariti.app

Table of Contents

Introduction

All security incidents must be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences for the services offered and the customers are limited. This document sets out the CCE Technologies Inc. plan for reporting and dealing with security incidents as related to the software application Clariti hosted at www.clariti.app , hereinafter “Clariti' or 'Service'.

What is a Security Incident?

A Security Incident means any incident that occurs by accident or deliberately that impacts the Service's communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or application services in Clariti. This includes unauthorized access to, use, disclosure, modification, or destruction of data or application services used or provided by Clariti.

An 'Account Data Compromise' is a security incident specific to Clariti user account data. It is an event that results in unauthorized access to or exposure of user's data stored and managed by Clariti on its servers, including financial data or sensitive authentication data. If an unauthorized person obtains user data from the Service, they can use this data to commit fraud.

Recognizing a Security Incident

A security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within our environment, or that of our third party service providers.

We need to look out for any indications that a security incident has occurred or may be in progress, some of which are outlined below:

- Monitor excessive or unusual log-in and system activity, in particular from any inactive user login IDs (user accounts)
- Watch out for excessive or unusual remote access activity into the Service. This could be relating to our staff or our third party providers
- The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executables and programs. This could be on our networks or systems and includes web-facing systems.
- Hardware or software key-loggers found connected to or installed on systems
- Suspicious or unusual activity on, or behaviour of, Web-facing systems, such on as our ecommerce website
- Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain user data or other sensitive data

Security Incident Response Team

This security incident response plan must be followed by all personnel involved in operating the Service. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of CCE Technologies Inc, working with Clariti or our customers' data or on CCE Technologies Inc. premises. For simplicity, all of these personnel are referred to as 'staff' within this plan.

Roles

The Clariti Security Incident Response Team (SIRT) is comprised of:

Role*	Responsibility	Name	Email
Information Security Officer	Incident Response Lead	Kishore S.N.	kishore@clariti.app
Systems & Risk Assessment Manager	Incident Response Technical Lead	Jayaraj R.	jayarajr@clariti.app
Software Systems	Updating software to address incident	Kiran Kumar B.	kiran@clariti.app
Senior Management Primary Contact	Executive Officer/Risk Owner	Kumar Rajan	rajank@clariti.app
Responsible For Communications	Handling of any external communications in relation to an incident	Debankan Chattopadhyay	debankan@clariti.app
Responsible For Legal Issues	Handling of any legal questions/issues relating to security incidents	Kumar Rajan	rajank@clariti.app
AWS (Hosting Providers) Liaison	Handling all communications with Amazon	Raja	rajar@clariti.app

Responsibilities

The Incident Response Lead is responsible for:

- Making sure that our Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained, at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties, including legal representation, law enforcement, etc. as is required.
- Authorising on-site investigations by appropriate law enforcement or security/forensic personnel, as required during any security incident investigation. This includes authorising access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include third party service providers, service partners, customers, etc., as required.
- Assisting law enforcement and security personnel during the investigation processes. This includes any forensic investigations and prosecutions.

- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future.
- Determine whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Reporting any security related issues or concerns to line management, or to a member of the SIRT.
- Complying with the security policies and procedures of Clariti. This includes any updated or temporary measures introduced in response to a security incident (e.g. for service continuity, incident recovery or to prevent recurrence of an incident).

External Contacts

External Party	Contact Name (if known)	Email
Fraud And Cyber-Crime Reporting Organisation – USA	CISA reporting forms:	https://www.us-cert.gov/forms/report

Incident Response Plan Steps

There are a number of steps and stages that you must be taken to make sure that you protect the Service by reacting to a security incident appropriately.

Report

- Information security incidents must be reported, without delay, to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).

- The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.
- In the event that a security incident or data breach is suspected to have occurred, the staff member should discuss their concerns with their line manager, who in turn may raise the issue with a member of the SIRT.

Investigate

- After being notified of a security incident, the SIRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Security Incident Response Plan.
- If the Security Incident Response Plan is initiated, the SIRT will investigate the incident and initiate actions to limit the exposure of user data and in mitigating the risks associated with the incident.

Initial Incident Containment and Response Actions

Access to Compromised Systems

- Isolate compromised systems from our network and unplug any network cables – without turning the systems off.
- Restrict the network access point and other systems that may be using this network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g. logs from firewall, anti-virus tool, access control system, web server, application server, database, etc.
- Perform a back-up of our systems to preserve their current state – this will also facilitate any subsequent investigations.
- Keep a record of all actions all members of the SIRT take.
- Stay alert for further indications of compromise or suspicious activity in our environment, or that of our third parties.
- If you can, gather details of all compromised or potentially compromised user accounts (the 'accounts at risk').

Inform

Once the SIRT has carried out their initial investigation of the security incident:

- The Incident Response Lead will alert the SIRT's senior management primary contact.
- The Incident Response Lead and / or the SIRT personnel responsible for communications / PR will inform all relevant parties. This includes management and local law enforcement, and other parties that may be affected by the compromise such as the customers, service partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

Service Continuity

The SIRT will engage with operational teams to make sure that the Service can continue to operate while the security incident is being investigated.

- Make sure you have system and data backups available in the event of loss of data, system corruption/virus infection or hardware failure.
- Consider what offline or methods could be used if users are unable to access the Service

Resolve

- The SIRT will liaise with external parties, including consultants, law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, as is required.
- The members of the SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.
- The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders (including management, local law enforcement, etc.) as is needed.

Recovery

- The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed.
- The SIRT will notify the rest of the staff and stakeholders that normal Service operations can resume.

- Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

Review

The SIRT will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled, to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Security Incident Response Plan and associated procedures.
- Updates to the Service's security or operational policies and procedures.
- Updates to technologies, security measures or controls
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).
- The SIRT Executive Officer/Risk Owner (the senior management primary contact) will ensure that the required updates and changes are adopted or implemented as necessary.

Specific Incident Response Types

Some specific incident types requiring additional response actions are provided below.

Malware (or Malicious Code)

- Disconnect devices identified with malware from the network immediately.
- Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device.
- Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.
- If the malware cannot be removed from the device rebuild using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware.

- Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

Unauthorized Web Access Points

If unauthorized web access points are detected, or reported by staff, these must be recorded as a security incident.

- SIRT will investigate to identify the location of the unauthorized web access points.
- The SIRT will investigate as to whether or not the unauthorized web-facing access point is being used for a legitimate Service purpose/need. If a legitimate Service reason is identified, then this web-facing access point must be reviewed and go through the correct management approval process. This is to make sure that the Service justification is documented and the access point is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
- All other unauthorized web-facing access points must be located, shutdown and removed.

Loss of Equipment

- The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the SIRT, management local law enforcement. This includes losses/thefts outside of the Service hours and at weekends.
- If the device that is lost or stolen contained sensitive user data, and the device is not encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen.
- Where possible, SIRT will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

Non Compliance with our Security Policy

This covers incidents resulting from deliberate or accidental actions that are in breach of our security policy and which put sensitive user data at risk. This includes any systems or data misuse, unauthorized exposure of data to external parties, unauthorized changes to systems or data.

- SIRT will engage with the relevant Service area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
- SIRT and/or line managers will notify Human Resources of the incident.
- SIRT will liaise with Human Resources and line managers to determine whether disciplinary action is needed.
- SIRT will undertake an assessment of the impact and provide advice and guidance to the Service area to prevent reoccurrence, for example re-training of staff.

Testing and Updates

Annual testing of the Incident Response Plan using walk-throughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

- The Incident Response Plan will be tested at least once annually.
- The Incident Response Plan Testing will test the Service response to potential incident scenarios to identify process gaps and improvement areas.
- The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
- The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

Document Control

Document Name:	Security Incident Response Plan
Current Version:	2020-0412
Plan Owner:	Kishore S.N.
Plan Approver:	Kishore S.N.
Date of Last Review:	04/15/20