Computer Incident Response Policy

2022

8. COMPUTER INCIDENT RESPONSE POLICY

POLICY STATEMENT

Citadel Servicing Corporation will take reasonable and appropriate steps to report, mitigate, and document computer, IT, and cyber security incidents and violations that impact company information systems, operations, and assets.

Company computer incident response policies and procedures will provide technical and managerial guidance to facilitate and govern recovery from incidents while striving to minimize operational impact, loss, or theft of company and client information.

All IT incidents must be immediately reported and assessed to determine the impact, severity, and the response required. Incident responses must follow established corporate procedures to ensure the incident is addressed and standards are followed. The procedures and standards are to:

- Ensure the restoration and recovery of services and data.
- Provide a root cause analysis to address the event and vulnerabilities.
- Mitigate or prevent recurrence of previously identified issues.
- Documentation of event and collection of evidence.

8.1. OVERVIEW

It is important for Citadel Servicing Corporation to identify, guide, and respond to suspected or known security incidents, manage any negative impacts, document incidents, and their outcomes. The resulting documentation may be used to implement remedial action, new safeguards, and report the incident to the appropriate local, state, and federal authorities/agencies as required by law/statute/regulation.

A. **Reporting an IT incident** — All IT incidents must be reported to IT Service Desk upon detection.
B. **Responding to an IT incident** — Personnel and groups have been identified for roles and responsibilities regarding the reporting and handling of IT incidents. All IT incidents must be assessed by the Information Technology and Security Office/ Leadership and Computer Emergency Response Team regarding impact, severity, and the response required.
C. **Documentation** — All documentation must follow established procedures in the Incident Response and Reporting System. All IT Incident documentation must be completed and reviewed.

8.2. PURPOSE

Citadel Servicing Corporation will take reasonable and appropriate steps to ensure that an Incident Response and Reporting System will be implemented and maintained to report, mitigate, and document IT and security incidents and violations.

The purpose of this policy is to provide technical and managerial guidance in efforts to:

- Enable quick and efficient recovery from IT (including security) incidents.
- Respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident, prevent or minimize disruption of critical computing services, recover and prevent the incident(s) from re-occurrence.
- Minimize negative impacts to systems and sensitive or mission critical information.

8.3. SCOPE

This policy applies to all employees, contractors, consultants, temporary employees, and other entities at Citadel Servicing Corporation including all personnel affiliated with third parties who process, store, transmit, or have access to company information and computing resources.

8.4. POLICY

It is the policy of Citadel Servicing Corporation to identify and respond to IT system and suspected or known information security incidents, mitigate as possible any harmful effects, and document such incidents and their outcomes. If the incident is classified as a security breach, Citadel Servicing Corporation may be required to report the breach to the appropriate local, state, and federal authorities or agencies.

It is the policy of Citadel Servicing Corporation to require employees to report any suspected or known security incidents to the service desk, their managers, and the Citadel Servicing Corporation Information Security Office Program Organization.

A. **Computer Emergency Response Plans** — For computer and communications systems, management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical systems in the event of an interruption or degradation of service.
B. **Incident Response Plan** — Citadel Servicing Corporation 's incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners (e.g., payment card issuers, suppliers, clients, vendors).
C. **Computer Emergency Response Team** — The Information Security Office must organize and maintain an in-house computer emergency response team (CERT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer-related emergencies such as virus infestations and hacker break-ins.
D. **IT Forensic Readiness Planning** — Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs. By having IT Forensic Readiness procedures in place, the company can make use of digital evidence when required. The goal of forensic readiness procedures is to maximise the company's ability to gather and use digital evidence whilst minimising disruption and/or cost.

8.4.1. Basic Guidelines

Citadel Servicing Corporation has implemented a Computer Incident Response and Reporting System which is reviewed on a regular basis by the Citadel Servicing Corporation Information Security Office. The plan includes the following:

- Systems, devices, and applications to be monitored.
- Incident reports for each system.
- Risk and threat analysis against systems and information.
- Procedures to review all incident reports and activity reports.
- A procedure for investigation, reporting, response activation for potential breach incidents escalation, and follow up if a breach is confirmed.

Citadel Servicing Corporation is responsible for systems containing company and client data and must therefore take steps to utilize a mechanism to log and store system incidents.

Incident reports must include, but are not limited to the following:

- Attack ID
- Incident Date/Time
- Actions taken
- Affected systems
- System and application log-in reports
- Exception reports
- Documented and implemented countermeasure activity

The Citadel Servicing Corporation Information Security Office must take steps to ensure that employees are provided training and awareness as defined in the Security Awareness policy.

8.4.2. Roles and Responsibilities

Each staff member has responsibilities related to the security of all Citadel Servicing Corporation computing systems and networks which include the reporting and handling of information security incidents. It is important for each entity to know designated roles and responsibilities.

A. The Company — Citadel Servicing Corporation must take reasonable steps to ensure that its employees are aware of policies, protocols, procedures and legal obligations relating to forensic readiness.

B. CSC Executive Team — Provides oversight activities for information security activities, including final approval of this policy.

C. Management Team — Managers are responsible for ensuring that their service operates within the corporate information security program framework. Along with ensuring the allocation of sufficient resources, they must ensure that:

- There are effective methods for communicating Information Security Program related issues within their service.
- Employees complete relevant training, and mandatory updates in relation to the company's Information Security Program and Security Awareness Policy.

D. Information Security Office — The Citadel Servicing Corporation Information Security Office is responsible for managing information security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of the supported IT systems. The Information Security Office:

- Serves as the focal point for reviewing information system security issues.
- Prepares guidelines for establishing and maintaining the security incident response plan.
- Handles and investigates all information security problems/incidents.
- Works with information security SMEs/liaisons to analyze and resolve security incidents.
- Coordinating the development and maintenance of IT forensic policy procedures and standards for Citadel Servicing Corporation .
- Evaluates and documents investigation findings after resolving an incident.
- Monitors performance through quality control and internal audits, identifying where improvements could be made.
- Recommends security strategies to appropriate executive management.
- Promotes security awareness to the Citadel Servicing Corporation computing community.

E. Information Security Office — The Citadel Servicing Corporation Information Security Office is responsible for:

- Coordinating the overall response and recovery activities for security incidents.
- Providing guidance and assistance in determining the appropriate action taken.
- Updating management of incident investigation findings.

F. **Human Resources** — Responsible for the distribution of IS policies, verifying user comprehension and agreement to policies through the collection of any associated statements of understanding.

G. **Technical Support Services** — Central Point of Contact for IT Requests and Security Violations.

H. **System Administrators** — System Administrators are familiar with all corporate systems and may often be the first to discover a security incident. System administrators are responsible for reporting incidents to the Information Security Office immediately, and when applicable, help determine and implement a solution. System Administrators should perform the following if there is a suspicion of a security incident:
   - Investigate.
   - If suspicion is confirmed or indeterminate, confer with supervisor, networking manager/administrator, and notify the Information Security Office immediately.
   - Start an event log by noting date and time of all actions.
   - Take snapshot of pertinent files within the first half hour of incident investigation and store original files (working of copies to maintain original evidence).
   - Implement appropriate measures (isolate, contain, remediate, and recover).

I. **Employees** — Any user who is directly employed by the organization. The majority of employees handle information in one form or another. Employees that in the course of their work create, use or otherwise process information have a duty to keep up to date with, and adhere to, relevant legislation, case law and industry regulations and guidance.

   Citadel Servicing Corporation policies and procedures reflect such guidance and compliance with these strategies and ensure a high standard of compliance within the organisation. All employees and management, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of the company's Information Security Program.

   All employees are required to assist in the identification of any information security issues / breaches and bring them to the attention of the Information Security Office and their relevant manager.

J. **Users** — Any user of the organization's IT assets, information assets, or facilities including hardware, software, network, components or any combination thereof. Despite advances in automated intrusion detection/prevention systems, computer users may be the first to discover an incident/intrusion. All users should:
   - Be vigilant for unusual system behavior that may indicate a security incident in progress.
   - Report suspected or known incidents (e.g., a virus infection, a system compromise, or a denial-of-service incident) to their manager and/or the Information Security Office.
   - Cooperate with investigative personnel during investigation as needed.

K. **Vendors** — Any user who is not directly employed by the organization including but not limited to service providers, business partners, suppliers, contractors, volunteers, or agents.

Incident Response Availability — The Citadel Servicing Corporation Computer Emergency Response Team must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

Designated Contact Person for All Disasters And Security Events — Unless expressly recognized as an authorized spokesperson for Citadel Servicing Corporation , no employee may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

Incident Management Responsibilities — The individuals responsible for handling information systems security incidents must be clearly defined by the Information Security Office. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

Providing Information In Legal Proceedings — Employees are prohibited from providing any company records, or any copies thereof, to third parties outside of Citadel Servicing Corporation or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of corporate Legal Counsel has first been obtained. Likewise, employees are prohibited from testifying to facts coming to their knowledge while performing in their official Citadel Servicing Corporation capacities, unless the prior permission of corporate Legal Counsel has first been obtained.

Criminal Justice Community Contact — Technical information systems staff must not contact the police or other members of the criminal justice community about any information systems problems unless they have received permission from corporate Legal Counsel.

Crisis Management Plan — The Physical Security Manager must organize and supervise a crisis management team. This team must prepare and annually update a crisis management plan which covers topics such as a process for managing the crisis, crisis decision making continuity, the safety of employees, damage control, and communications with third parties such as the media.

Display of Incident Reporting Contact Information — Citadel Servicing Corporation contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters and the intranet.

8.4.3. Procedures

A. **Incident Response Plan – Procedures** — The Citadel Servicing Corporation incident response plan must include specific incident response procedures.
B. **Incident Response Plan – Legal Requirements** — The Citadel Servicing Corporation incident response plan must include analysis of legal requirements for reporting compromises.
C. **Incident Response Plan – External Partners** — The Citadel Servicing Corporation incident response plan must include reference or inclusion of incident response procedures from relevant external partners (e.g., payment card issuers, suppliers).
D. **Annual Incident Response Testing** — At least once every year, the Information Security Office must utilize simulated incidents to mobilize and test the adequacy of the company's Computer Emergency Response Team (CERT).
E. **Problem Reporting** — A formal information systems problem management process must be both established and operational in order to record the problems encountered, reduce their incidence, and to prevent their recurrence.
F. **Security changes after system compromise** — Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, System Administrators must immediately reload a trusted version of the operating system and all security-related software, and all recent changes to user and system privileges must be reviewed for unauthorized modifications.
G. **Extended Investigations** — Extended investigations of security breaches must be performed while the suspected employee is given leave without pay. The reason for a suspect's leave without pay must not be disclosed to co-workers without the express permission of company management.
H. **Suspected System Intrusions** — Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and predetermined procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

I. **Intrusion Response Procedures** — The Information Security Office must document and periodically revise intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

J. **Unauthorized Access Problems** — Whenever unauthorized system access is suspected or known to be occurring, Citadel Servicing Corporation personnel must take immediate action to terminate the access or request assistance from Technical Support Services.

K. **Information Security Problem Resolution** — All information security problems must be handled with the involvement and cooperation of in-house information security staff, the Citadel Servicing Corporation Computer Emergency Response Team, or others who have been authorized by the company's Information Security Office.

L. **Violation and Problem Analysis** — An annual analysis of reported information security problems and violations must be prepared by the Information Security Office.

M. **Law Enforcement Inquiries** — Even if the requesting party alleges to be a member of the law enforcement community, Citadel Servicing Corporation employees must not reveal any internal company information through any communications mechanism unless they have established the authenticity of the individual's identity and the legitimacy of the inquiry.

N. **Legal Proceeding Participation** — Any Citadel Servicing Corporation employee called by a subpoena or in any other manner called to appear or testify before a judicial board or government agency must immediately notify the chief legal counsel in writing about the call.

O. **Receiving reports of identity theft from customers** — Citadel Servicing Corporation must establish documented procedures for receiving reports from customers concerning fraud or other compromise of customer data. These procedures must be displayed on the Citadel Servicing Corporation web site.

8.4.4. Event Monitoring

A. **Incident Alerts – IDS** — The incident response plan must include actions required to alerts from the intrusion detection system.

B. **Incident Alerts – IPS** — The incident response plan must include actions required to alerts from the intrusion prevention system.

C. **Incident Alerts – File Integrity Monitoring Systems** — The incident response plan must include actions required to alerts from all file integrity monitoring systems.

D. **Incident Alerts – Wireless Access Points** — The incident response plan must include actions required to alerts from wireless access point monitoring.

E. **Monitoring and Recording Usage of Shared Computing Resources** — The usage of all Citadel Servicing Corporation shared computing resources employed for production activities must be continuously monitored and recorded. This usage history data must in turn be provided in real-time to those security alert systems designated by the Information Security Office (intrusion detection systems, virus detection systems, spam detection systems, etc.).

F. **Intrusion Detection Systems** — On all internal servers containing confidential and secret data, Citadel Servicing Corporation must establish and operate application system logs, intrusion detection systems, and other unauthorized activity detection mechanisms specified by the Information Security Office.

8.4.5. Reporting Information Security Events

A. **External Violation and Disclosure Reporting of Computer System Attacks** — Where required by industry regulations, state and federal laws and statutes to report information security violations to external

authorities, senior management, in conjunction with representatives from the Legal Department, the Information Security Office, and the Physical Security Department will review all information before disclosure and reporting of any violations to the public or any government agencies.

***Note:** California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) [agency] and California Civ. Code s. 1798.82(a) [person or business]).

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (California Civil Code s. 1798.29(e) [agency] and California Civ. Code s. 1798.82(f) [person or business]) (http://oag.ca.gov/ecrime/databreach/reporting).

B. PII Data — If a security incident occurs that involves PII data, Citadel Servicing Corporation is required to notify appropriate data partners within twenty-four (24) hours of the incident involving their data.

C. Loss or Disclosure of Sensitive Information — If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Office must be notified immediately.

D. Off-Site Systems Damage and Loss — Employees must promptly report to their manager any damage to or loss of Citadel Servicing Corporation computer hardware, software, or information that has been entrusted to their care.

E. Incident Reporting — All suspected information security incidents must be reported as quickly as possible through the approved Citadel Servicing Corporation internal channels.

F. Incident Reporting Severity — Any incident which might reasonably be expected to lead to further losses, no matter how insignificant its present loss, must be reported to the Information Security Office.

G. Violation and Problem Reporting Alternatives — Citadel Servicing Corporation employees must immediately report all suspected information security problems, vulnerabilities, and incidents to either their immediate manager, Technical Support Services or to the Information Security Office.

H. Reporting Security Breaches to Third Parties — If an information systems security breach at Citadel Servicing Corporation causes private or proprietary third-party information to be exposed, then these same third parties must be notified immediately so that they can take appropriate action.

I. Reporting Suspected Security Breaches to Third Parties — If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

J. Reporting Unauthorized Activity — Users of Citadel Servicing Corporation information systems must immediately report to their Cognizant Manager or the Information Security Office any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported.

K. Reporting Unexpected Requests for Log-In Information — Other than the regular and expected Citadel Servicing Corporation log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for an Citadel Servicing Corporation user ID and password. Users encountering these requests must refrain from providing their company user ID and password, as well as promptly report the circumstances to Technical Support Services.

L. Contacting Law Enforcement — Every decision about the involvement of law enforcement with information security incidents or problems must be made by an Citadel Servicing Corporation corporate

officer. Likewise, every contact informing law enforcement about an information security incident or problem must be initiated by a corporate officer.

M. **Requests to Cooperate in Investigations** — Citadel Servicing Corporation employees must immediately report every request to participate in an information security investigation to the Chief Legal Counsel. Any sort of cooperation with the requesting party is prohibited until such time that the Chief Legal Counsel has determined that the participation is legal, is unlikely to cause problems for Citadel Servicing Corporation , and is requested by an authorized party.

N. **Reporting Unintended Sensitive Information Disclosures** — Unintended disclosures of sensitive Citadel Servicing Corporation information are serious matters, and they must all be immediately reported to both the Chief Legal Counsel and the Information Security Office. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

O. **Reporting of Software Malfunctions** — All apparent software malfunctions must be immediately reported to line management or the information system service provider.

P. **Unauthorized Wireless Access Point Notification** — If an unauthorized wireless access point is detected on the Citadel Servicing Corporation network the Information Security Office must be notified.

8.4.6. Reporting Security Weaknesses

A. **System Problem Notification** — Systems designers and developers are individually responsible for notifying project management about any problems that might be caused by the applications they are building or modifying.

B. **Disclosure of Information System Vulnerabilities** — Specific information about information system vulnerabilities, such as the details of a recent system break-in, must not be distributed to persons who do not have a demonstrable need to know.

C. **Public Releases of Vulnerability Information** — Press releases or other public statements issued by Citadel Servicing Corporation containing information systems vulnerability information must be free of explicit details.

D. **Production System Problems** — All significant errors, incomplete processing and improper processing of production applications must be promptly reported to Technical Support Services.

E. **Reporting System Vulnerabilities** — Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to Technical Support Services or Information Security Office. Users are prohibited from utilizing Citadel Servicing Corporation systems to forward such information to other users, whether the other users are internal or external to the company.

F. **Reporting Security Vulnerabilities** — When a new and serious information systems security vulnerability associated with a particular vendor's hardware or software is discovered, it must be immediately reported to appropriate public forums for public dissemination.

G. **Integrity Controls Failure Notification** — If controls that assure the integrity of information fail, if such controls are suspected of failing, or if such controls are not available, management must be notified of these facts each time they are presented with the involved information.

H. **Disclosure of Software Vulnerabilities by Researchers** — Citadel Servicing Corporation encourages security researchers to responsibly disclose vulnerabilities discovered within its web site or application software. Citadel Servicing Corporation will not take legal action against researchers that disclose software flaws directly to the company at least 90 days before any public disclosure.

8.4.7. Data Breach Management

A. **Data Breach Response Plan Required** — Citadel Servicing Corporation management must prepare, test and annually update a Data Breach Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

8.4.8. Incident Review

A. **Incident Response Plan Evolution – Lessons Learned** — The incident response plan must be updated to reflect the lessons learned from actual incidents.
B. **Incident Response Plan Evolution – Industry Developments** — The incident response plan must be updated to reflect developments in the industry.
C. **Computer Crime or Abuse Evidence** — To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The relevant information must then be securely stored off-line until official custody is given to another authorized person or the chief legal counsel determines that Citadel Servicing Corporation will no longer need the information. The information to be immediately collected includes the current system configuration as well as backup copies of all potentially involved files.

8.4.9. Collection of Evidence

A. **Sources of Digital Evidence** — For every production computer system, the Information Security Office must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subjected to a standardized capture, retention, and destruction process comparable to that used for vital records.
B. **Disclosure of Information to Law Enforcement** — By making use of Citadel Servicing Corporation systems, users consent to allow all information they store on corporate systems to be divulged to law enforcement at the discretion of Citadel Servicing Corporation management.
C. **Special Data classification for possible electronic evidence** — Citadel Servicing Corporation data that may be considered electronic evidence must have a specific data classification. An electronic evidence handling policy, published jointly by the information security department and the legal department, will outline the controls required to protect this special class of data.

8.4.10. Investigation and Forensics

1. **Forensic Analysis Process** — Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.
2. **Investigation Status Reports** — The status of information security investigations must be communicated to management only by the lead investigator or the management representative of the investigation team.
3. **Computer Crime Investigation Information** — All evidence, ideas, and hypotheses about computer crimes experienced by Citadel Servicing Corporation , including possible attack methods and perpetrator intentions, must be communicated to the Chief Legal Counsel and treated as restricted and legally privileged information.
4. **Information Security Investigations** — All Citadel Servicing Corporation internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Office.
5. **Intrusion Investigations Details** — Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of intruders, files which describe an investigation now underway must not be stored on potentially

compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

8.5. IT FORENSICS READINESS

Forensic readiness is the ability of an organisation to make use of digital evidence when required. It is a key component in the management of information risk with the goal of maximizing the company's ability to gather and use digital evidence whilst minimising disruption and/or cost.

IT Forensic Readiness Planning is proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs.

Citadel Servicing Corporation acknowledges that IT forensics provides a means to help prevent and manage the impact of important business risks. IT Forensics evidence can support a legal defence, it can verify and may show that due care was taken in a particular transaction or process and may be important for internal disciplinary actions.

Examples of business scenarios when digital forensics may be required, and what evidence may be required are:

- Employee internet misuse / abuse.
- Employee email misuse / abuse.
- Employee performance issues.
- Electronic bullying / harassment.
- Formal Police / legal request for digital evidence.
- Social networking evidence.
- Fraud.
- Security camera and CCTV footage.
- Production of audit logs.
- Back up data.
- Removal media.
- Network intrusion / prevention audit records such as cyber-attacks (e.g., hacking attempts).
- Mobile phone and desk phone investigation.

The purpose of having IT forensics readiness procedures in place is to assist Citadel Servicing Corporation to:

- Meet industry and legal standards and requirements relating to the security and confidentiality of equipment and information.
- Set out procedures to be followed where an area of criminal activity is determined, particularly where there is suspicion of a breach to corporate data systems where information is potentially compromised.
- Protect Citadel Servicing Corporation , its employees, partners and its clients through the availability of reliable digital evidence gathered from its systems and processes.
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to Citadel Servicing Corporation business and operations.
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
- Demonstrate due diligence and good governance of Citadel Servicing Corporation 's information assets.

The benefits to the organisation of having IT forensic readiness procedures in place are that they:

- Act as a deterrent to insider threats.

- Enable minimum disruption in the event of an incident and links into the Citadel Servicing Corporation Business Continuity plans.
- Reduce cost and time of internal investigations.
- Extend information security to the wider threat from cyber-crime.
- Demonstrate due diligence and good enterprise governance arrangements.
- Ensure compliance with industry and other regulatory requirements.
- Improve the prospects for successful legal action if required.
- Support employee sanctions based on digital evidence.

8.6. ENFORCEMENT

All users (employees, contractor, part-time and temporary employees) and those employed by others to perform work for the organization, or who have been granted access to IT assets or facilities, are covered by this policy, and must comply with its associated policies, procedures, standards and guidelines.

Failure to comply with this policy and associated guidelines may result in suspension of use privileges or other disciplinary actions up to and including termination and/or legal action.