Document # SEC-POL-010

Security Incident Response Policy

Version 6.0

Document Owner: Kony CISO

Status: Approved

Kony Inc.

Document control:

Kony Entity	Kony Inc.
Document Number	SEC-POL-010
Document Title	Security Incident Response Policy
Document Owner	Kony CISO
Document Status	Approved
Current Version	6.0
Security Classification	Kony Confidential

Document Change log:

Date	Previous Version	New Version	Author	Change Log
4-Aug-2019	5.0	5.01	Srikrishan Gaddam	• Policy revamp of older "Incident Management CAPA Procedure". • Repetitive sections have been removed. • Consolidation of relevant sections in a concise manner. • New policy template applied • Clarity in roles and responsibilities fine-tuned, definition of newer roles for incident handling to reflect the current security environment.

Review log:

Date	Version reviewed	Reviewed by	Reviewer's Designation
5-Aug-2019	5.01	Brian Rutledge	Sr. Director of Corporate Compliance

Approvals & Sign-offs:

Date	Version	Approver Name	Title
29-Sep-2019	6.0	Brian Rutledge	Sr. Director of Corporate Compliance

Table of Contents

1. PURPOSE

This policy defines the requirements for reporting and responding to incidents related to Kony information systems and operations.

2. SCOPE

This policy applies to all employees and partners of Kony entities including, but not limited to, business units and subsidiaries.

3. POLICY

3.1 Program Organization

Security Emergency Response Plans - Kony management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service.

Incident Response Plan Contents - The Kony incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners. Specific areas covered in the plan include:

- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Identification and coverage for all critical system components.
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers.

3.2 Security Emergency Response Team (SERT)

Security Emergency Response Team - Kony must organize and maintain an in-house inter-departmental Security Emergency Response Team (SERT) 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.

Incident Response Team Availability - The Kony Security 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.

3.3 Information Security Incident – Definition

"Security Incident" is an adverse event that has caused or has the potential to cause damage to an organization's assets, reputation and/or users. Incident management is concerned with intrusion, compromise or damage to any asset and the continuity of critical information systems and processes.

Few examples of Information Security Incidents are:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without appropriate knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- Unauthorized use of a system for the processing or storage of data by any person.
- Computer system breach.
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data.
- Denial of service attack.
- Interference with the intended use of IT resources.
- Compromised user accounts.

3.4 Events and Incidents to Report

Off-Site Systems Damage and Loss - Workers must promptly report to their manager any damage to or loss of Kony computer hardware, software, or information that has been entrusted to their care.

System Alerts and Warnings - Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Systems Help Desk. Users are prohibited from utilizing Kony systems to forward such information to other users, whether the other users are internal or external to Kony.

Unauthorized Activity - Users of Kony information systems must immediately report to the Information Security Manager any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported to the same manager.

Unexpected Requests for Log-In Information - Other than the regular and expected Kony log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for a Kony user ID and password. Users encountering these requests must refrain from providing their Kony user ID and password, as well as promptly report the circumstances to the Help Desk.

Missing Access Devices - Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Information Security Department immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords,

telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported immediately.

Unintended Sensitive Information Disclosures - Unintended disclosures of sensitive Kony information are serious matters, and they must all be immediately reported to both the Chief Legal Counsel and the Information Security Manager. 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.

Software Malfunctions - All apparent software malfunctions must be immediately reported to line management or the information system service provider.

Unauthorized Wireless Access Points - If an unauthorized wireless access point is detected on the Kony network the Computer Incident Response Team must be notified.

3.5 Recognizing and Classifying a Security Incident

The events and incident that eventually are confirmed as clear case violation of Kony Security policies will be classified for the purposes of process improvements, knowledge enhancements, documentation and monitoring:

- Policy violation – actions and/or events that are in direct contradiction of laid organisational policies.
- Social engineering – the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Remote attack – is a malicious action that targets one or a network of computers. The remote attack does not affect the computer the attacker is using. Instead, the attacker will find vulnerable points in a computer or network's security software to access the machine or system. These attacks originate outside of Kony networks. The attacker manages to connect his/her machine to the network and takes advantage of bugs or weaknesses in the system.
- Local attack – the attacker has an account on the system in question and can use that account to attempt unauthorized tasks. These attacks typically originate within Kony facilities and environments.
- Advanced Persistent Threat (APT) - is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for a period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.
- Malware attack - is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- Fraudulent activity – is a deliberate or unlawful deception, misrepresentation or concealment of facts practiced to secure advantage, benefit or gain (including benefit to the Kony) and/or to cause loss to another. The intended benefit to be gained is usually financial or personal in nature.

  Fraud is a broad subject, hence for the scope of this policy, the fraudulent activities in the context of security incident are:

  - Phishing attack – is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

- Pharming – is a cyberattack intended to redirect a website's traffic to another, fake site.

3.6 Reporting the Information Security Incidents

3.6.1 Incident Reporting

All suspected information security incidents must be reported as quickly as possible through the approved Kony internal channels.

- The e-mail id for reporting security incidents in Kony is sirteam@kony.com. Users must report security incidents by sending e-mail to the aforementioned email ID.
- The e-mail id for reporting security incidents must be communicated to all Kony workers, staff, employees and contractors.
- The new joiners must be made trained at the time of induction on how to report security incidents.
- The users should be warned not to attempt to resolve any incident on their own. The same shall be considered as breach of security and may form a base for disciplinary actions.
- The users, in the case of reporting any security incidents are expected to contain the incident from causing further damage to the extent possible. E.g. if user suspects that the computer is infected by a virus, the computer should be disconnected from the network and should not be plugged back till clearance is obtained from the ITS Helpdesk for usage of the computer.

3.6.2 Security Incident Alerting Systems and Mechanisms

Information Systems groups and departments that administer, manage and support IT systems and infrastructure must establish, maintain, and periodically test a communications system permitting workers to promptly notify appropriate staff about suspected information security problems.

3.6.3 Policy Violation Incidents – Alternative Reporting Channels

Kony workers must immediately report all suspected information security problems, vulnerabilities, and incidents to either their immediate manager or to the Information Security Group.

Also, refer the document: "Kony – Fraud Risk Management Policy"

3.6.4 Policy Violation Incidents – Reporting Protection

Kony will protect workers who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. This means that such workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

Also, refer the document: "Kony – Fraud Risk Management Policy"

3.6.5 Policy Violation Incidents – Privacy Protections for Reporting

Workers who report to the Information Security Department a security problem, vulnerability, or an unethical condition within Kony may, at their sole discretion, have their identity held in strict confidence. This means that the whistleblower's immediate supervisor, other members of the management team, as well as other Kony workers who are not directly involved in the receipt of the report, will not be given the whistleblower's identity.

Also, refer the document: "Kony – Fraud Risk Management Policy"

3.7 Incident Handling, Response and Recovery

3.7.1 Preliminary Incident Handling

If the reported issue qualifies for an Incident, a mail must be sent by the Security Incident Response Team's representative to the relevant personnel/department who will attempt to resolve the problem with minimum details of the incident like:

- Date and time of incident.
- Names of information system components (e.g. systems, programs or networks) that have been affected.
- Email address
- Description of the information security problem.

If the problem remains unresolved within defined timeframe, Security Incident Response Team will escalate the incident as per Appendix A. Once the problem is resolved, a mail should be sent to all parties involved notifying the same.

3.7.2 Incident Response Procedures – Corrective and Preventive Actions

The process for corrective/preventive action shall be initiated whenever a condition warrants an investigation for a qualified incident. Corrective and Preventive action shall be documented using the incident report and processed electronically in accordance with this document.

Corrective and Preventive action shall be initiated as a result of security incidents which may be reported because of, but not limited to the following:

- Internal and external audits;
- Customer reported security incidents
- Vulnerability Assessment & Penetration Testing
- Risk Management and Business Impact Analysis
- Problems identified by Kony users pertaining to security weaknesses
- Violation of security policy and security objectives
- Notifications from Security Newsletters / Bulletins

3.7.3 Intrusion Response Procedures

Information Systems groups and departments that administer, manage and support IT systems and infrastructure 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.

3.7.4 Information Security Problem Resolution

All information security problems must be handled with the involvement and cooperation of in-house information security staff, the Kony Computer Emergency Response Team, or others who have been authorized by the Kony Information Security Department.

3.7.5 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.

3.7.6 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.

3.7.7 Unauthorized Access Problems

Whenever unauthorized system access is suspected or known to be occurring, Kony personnel must take immediate action to terminate the access or request assistance from the Corporate Information Systems Help Desk.

3.7.8 Internal Investigations Information Confidentiality

Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

3.7.9 Legal Proceeding Participation

Any Kony worker 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.

3.8 Roles and Responsibilities

3.8.1 Incident Management Responsibilities

The individuals responsible for handling information systems security incidents must be clearly defined in accordance with Kony's Information Security organization and policies. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

#	Incident Management Role	Responsibilities
1	Incident Reporter	• Must report a security incident in a timely manner with adequate information using the established incident reporting communication channels;

2	Security Emergency Response Team (SERT)	• SERT acting as "first person on-scene" will undertake preliminary handling procedures to gather information leading up to the incident manifestation;
		• Notifying appropriate Incident Response Teams about the incident;
		• Advising incident reporter procedures that will help minimise the impact of the ongoing security incident, if they can;
		• performs a follow-up verification to assess and determine its effectiveness of Corrective / Preventive Action Plan. Follow-up analysis must include the following:
		  • What has gone wrong leading security incident?
		  • Did detection occur promptly or, if not, why?
		  • Could additional tools have helped the detection and eradication process?
		  • Was the incident sufficiently contained?
		  • Was communication adequate, or could it have been better?

#	Incident Management Role	Responsibilities
		• What practical difficulties were encountered? • Was any hardware damaged?
3	Incident Response Teams	• Investigate the potential root-causes of the nonconformance/security incident; • Prepare and execute Corrective Action Plan that will provide short-term fix, which may fix the symptoms without proper diagnostics, when root-cause is not known. • Prepare and execute Preventive Action Plan that will provide permanent fix after undertaking diagnostic efforts to ascertain the root-cause of the issue. • Update the documented processes and procedures resulting from the Corrective / Preventive Actions execution. • Prepare and submit Incident Reporting form;
4	Incident Management Group	• Coordinate with internal and external teams, if applicable, and personnel until Corrective and Preventive action plans resolve the issue; • Act as the communication liaison for the involved parties in each incident; Communication of the changes • Appraise Kony management and Legal teams, if needed; • Provide training inputs to the affected individuals or business processes;

3.8.2 Designated Contact Person for All Disasters and Security Events

Unless expressly recognized as an authorized spokesperson for Kony, no worker 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.

3.8.3 Providing Information in Legal Proceedings

Workers are prohibited from providing any Kony records, or any copies thereof, to third-parties outside of Kony or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the Kony Legal Counsel has first been obtained. Likewise, workers are prohibited from testifying to facts coming to their knowledge while performing in their official Kony capacities, unless the prior permission of the Kony Legal Counsel has first been obtained.

3.9 Awareness and Training

Display of Incident Reporting Contact Information - Kony 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.

3.10 Event Monitoring

Monitoring and Recording Usage of Shared Computing Resources - The usage of all Kony 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 Department (intrusion detection systems, virus detection systems, spam detection systems, etc.).

Intrusion Detection Systems - On all internal servers containing sensitive data, Kony must establish and operate application system logs, intrusion detection systems, and other unauthorized activity detection mechanisms specified by the Information Security Department.

3.11 Reporting to Third-Parties

External Violation Reporting - Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with representatives from the Legal Department and the Information Security Department must weigh the pros and cons of external disclosure before reporting these violations.

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.

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 Department must be notified immediately.

System Vulnerability Exploitation and Victim Data - Kony staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly.

Vendor Vulnerability Disclosure - If a serious information system vulnerability is discovered by Kony workers, and the vulnerability can be directly traced to a weakness in a certain vendor's hardware and/or software, then that vendor must promptly and confidentially be notified of the problem.

3.12 Contact with Authorities

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 the Chief Legal Counsel.

Law Enforcement Inquiries - Even if the requesting party alleges to be a member of the law enforcement community, Kony workers must not reveal any internal Kony information through any communications mechanism unless they have established the authenticity of the individual’s identity and the legitimacy of the inquiry.

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems must be made by a Kony senior partner. Likewise, every contact informing law enforcement about an information security incident or problem must be initiated by the Information Security Manager.

Requests to Cooperate in Investigations - Kony workers 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 Kony, and is requested by an authorized party.

3.13 Data Breach Management

Data Breach Response Plan Required - Kony 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.

Link to Data Breach Management

3.14 Incident Review

Incident Response Plan - Lessons Learned - The incident response plan must be updated to reflect the lessons learned from actual incidents.

Incident Response Plan - Industry Developments - The incident response plan must be updated to reflect developments in the industry.

Violation and Problem Analysis - An annual analysis of reported information security problems and violations must be prepared by the Information Security Department.

3.15 Collection of Evidence

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 information to be immediately collected includes the current system configuration as well as backup copies of all potentially involved files.

Evidence Storage -The relevant information for computer investigation must then be securely stored off-line until official custody is given to another authorized person or the chief legal counsel determines that Kony will no longer need the information.

Sources of Digital Evidence - For every production computer system, the Information Security Department 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 subject a standardized capture, retention, and destruction process comparable to that used for vital records.

Responsibility for Electronic Evidence Production - Kony will appoint a single individual responsible for coordinating the discovery and presentation of electronic evidence that may be required to support litigation.

Information Classification - Kony data that may be considered electronic evidence must be classified as CONFIDENTIAL and viewed only by authorized representatives of the CERT or approved third parties involved in the investigation.

3.16 Investigation and Forensics

Computer Crime Investigation - Whenever evidence clearly shows that Kony has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Extended Investigations - Extended investigations of security breaches must be performed while the suspected worker 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 the Director of Security.

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.

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.

Computer Crime Investigation Information - All evidence, ideas, and hypotheses about computer crimes experienced by Kony, including possible attack methods and perpetrator intentions, must be communicated to the Chief Legal Counsel and treated as restricted and legally privileged information.

Information Security Investigations - All Kony internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Manager.

Information Security Investigation Teams - Any person who personally knows the suspects, or who is friendly with them, for conflict of interest reasons is barred from participating on an information security incident investigation team.

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.

4. VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Kony reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Kony does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Kony reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

5. DEFINITIONS

Event - An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Nonconformity - is the non-fulfillment of a specified requirement and may relate to a product requirement or to a process requirement.

Corrective Action - is undertaken to eliminate the cause of non-conformity/ security incident.

Preventive Action - is undertaken to eliminate the cause of a potential nonconformity / security incident in order to prevent occurrence.

Objective Evidence - Verifiable qualitative or quantitative information, observations, records or statements of fact pertaining to the quality of the product, process or system.

Root-Cause - A fundamental deficiency that results in a nonconformance which must be corrected to prevent recurrence of the same or similar nonconformance.

6. REFERENCES

ISO/IEC 27002: 16.0 Information Security Incident Management

NIST: Incident Response (IR)

HIPAA: Security Incident Procedures 164.308(a)(6)

PCI-DSS: 12.10 Incident Response Plan

7. RELATED DOCUMENTS

Appendix A – Incident Reporting Form

Reported By:	Date & Time of
Incident #:	Location:
Description of Incident:	
Incident Details forwarded to (i.e. Department Name):	Date & Time: / /
Analysis/Findings:	
Description of Root Cause(s):	
Description of Corrective Action:	Target Date (if not implemented):
Description of Preventive Action:	Target Date (if not implemented):
Description of Lessons Learnt:	Target Date (if not implemented):
Reviewed By:	Date: / /
Provide Documented Evidence of CAPA Implementation/ Effectiveness:	
Corrective and Preventative Action Status: Closed	Date: / /