Information Security Policy

Document Attributes

Contact Information

	Name
Owner	Jim Gasaway
Author	Chris Hyde

Approval History

Approver	Role	Document Version	Date	Approval
Jim Gasaway	Chief Technology Officer	4.2	09 Jan 2019	JMG

Revision History

Date	Version	Revised by	Description of Change
1/19/20	4.2	CJH	Annual Review, minor changes from prior version.
11/30 /2018	4.1	CJH	Add content from Kount Data Standard which is more relevant to Information Security; general updates
7/6/18	4.0	CJH	Various updates and General Review; updates for GDPR and California data privacy concepts
11/16 /2017	3.9	bkp	Revised approvers.
3/31 /2017	3.8	sam	Added encryption requirement for all removable media.
9/15 /2016	3.7	tja	Personal devices must not be jailbroken
9/7 /2016	3.6	tja	Badge and visitor log retention specified at least 365 days.
8/19 /2016	3.5	sam	Gramatical corrections and clarification on user account reviews.
1/24 /2016	3.4	sam	Minor edits and clarification on additional guidelines
2/27 /2015	3.3	sam	Imported into Confluence and minor updates to clarify policy for PCI 3.0
12/16 /2013	3.2	mdp	Annual review, formatting changes, Keynetics changed to Kount
11/23 /2012	3.1	rls	Annual review and revised approvers
9/14 /2011	3.0	rls	Revised references to Kount CTO
12/22 /2010	2.1	ajc	Added Privacy Policy as section 9.0
10/08 /07	2.0	jwm	Changed to Version 02.0
12/9/06	1.2	mw	Added requirement that all wireless networks require pre-approval of the CTO. Changed Revision History and Approval History to standard format.
9/14 /2006	1.1	rls	Minor grammar changes.

Tables of Contents

Document Sections

PCI References

PCI DSS Requirement	Related Document Sections
PCI_DSS_1.1	Information Security Policy#Information Security Policy

PCI_DSS_1.1.1.a	Information Security Policy#Configuration Management Policy
PCI_DSS_6.4	Information Security Policy#Segregation of Production Environment Information Security Policy#Appropriate Separation of Duties
PCI_DSS_12.1.1	Information Security Policy#Document Attributes
PCI_DSS_12.3.1	Information Security Policy#Acceptable Use
PCI_DSS_12.3.2	Information Security Policy#Wireless Access Points Information Security Policy#Remote Access
PCI_DSS_12.3.5	Information Security Policy#Wireless Access Points Information Security Policy#Personal Devices Information Security Policy#Modems
PCI_DSS_12.3.6	Information Security Policy#Wireless Access Points Information Security Policy#Personal Devices Information Security Policy#Modems
PCI_DSS_12.3.8.a	Information Security Policy#Modems
PCI_DSS_12.3.10.a	Information Security Policy#Remote Access
PCI_DSS_12.3.10.b	Information Security Policy#Remote Access
PCI_DSS_12.4.a	Information Security Policy#Guiding Principles

Introduction

Information is a core Kount asset. Reliable, timely access to accurate information is a fundamental business requirement. The proper protection of information and information security is part of everyone's job at Kount. This document, with supporting reference documents, explains how we will meet Kount's information security objectives.

Purpose

The Kount Information Security Policy (KISP) and other supporting documents are designed to ensure that security and control practices are implemented and effective. These practices are applied based on the value of the information assets, the risk associated with the assets, and the regulations pertaining to the information assets.

Information security is characterized by the following objectives:

- Confidentiality: ensuring that information is accessible only to those authorized to have access and that privacy is properly protected.
- Integrity: ensuring processes and procedures generate complete, consistent, and accurate data and that complete, consistent, and accurate data is preserved throughout the data life cycle
- Availability: ensuring that authorized users have timely and reliable access to information and associated assets when required.

Scope

This policy applies to all Kount information users including, but not limited to, employees, officers, members of the Board of Directors, agents, contractors, temporary staff, consultants, advisors and other parties employed by or contracted to Kount. This policy regulates users' access to, and use of, Kount information resources and the information resources of Kount affiliates. This policy applies to all equipment that is owned or leased by Kount. This policy may also cover access to Kount information resources by third parties.

Guiding Principles and Security Organization

Kount management will establish policies, standards, procedures, and guidelines to protect information resources and to comply with applicable laws and regulations. Kount management will also help ensure this policy is communicated to appropriate parties

Kount will employ a Security Management team as outlined in the Security Management Standard. Kount will provide adequate resources and executive support to ensure the Security Management team meets its objectives.

Risk Assessment and Policy Update

The Information Security team will coordinate an annual risk assessment catalog the current threats and vulnerabilities of the company's physical environment, networks, and computing resources. The risk assessment will also include an analysis of mitigating controls. Additional updates will be made in the event of major changes in the environment or business practices of the company.

Policy Review

This policy will be reviewed and reasserted at least annually.

Fundamental Policies

Build and Maintain a Secure Network

Kount will implement proper controls for company-owned networks and networks of company partners. Controls must be consistently applied across the information processing infrastructure. Controls applied will be proportionate to the value of the information assets contained within the system, associated risks with the system, and the regulations pertaining to the relevant information assets.

A secure network will use appropriate implementations of tools and techniques such as network segregation, traffic filtering, firewalls, access controls including enforced paths, authentication and routing**.**

For further details, see the Networking Device Policies.

Documented Operational Procedures

Operational procedures for the implementation and maintenance of systems, hardware and software must be defined to ensure compliance and data protection. The extent of procedural documentation will be based on the value of the information assets contained within the system, the risk associated with the system and the regulations pertaining to the relevant information assets.

Protect Stored Data

Appropriate controls will be implemented to protect stored data. When confidential data is stored controls such as encryption, access control, obfuscation and truncation will be employed as required.

Minimize Storage of Confidential Data

System designs will seek to minimize the storage of confidential data whenever possible. Storage of confidential data will be limited to that which is required for business, legal or regulatory purposes. Care must be taken when storing confidential data on desktop systems or in tangible form (i.e. paper documents, images, etc.). All confidential data should be protected and purged according to its classification.

For further details, see the Kount Data Standard.

Encryption Key Management

Kount must maintain strong operational procedures and guidelines related to managing encryption keys.

For further details, please refer to the **Data Encryption and Hashing Standard** and the **Encryption Key Custodian Duties**.

Information Transmission

Appropriate controls must be maintained over the electronic transport of information. Confidential Information traveling through any public network shall be encrypted according to the standards defined in the Data Encryption and Hashing Standard, section titled Acceptable Encryption.

The transmission of any cardholder data (encrypted or not), via email or any other end-user messaging technology, is strictly prohibited.

Intrusion Detection

Intrusion Detection System (IDS) software will be deployed on internal networks. The system will generate alerts for suspected compromises. Alerts will be investigated to evaluate the severity of the event and the scope of remediation, if needed.

Vulnerability Management Program

Kount will maintain and operate a vulnerability management program. This program will include regular preventative actions such as scanning, testing for and remediation of vulnerabilities. For further details related to vulnerability management, please refer to the Security Management Standard.

Incident Response Capability

Kount must maintain the capacity to prevent, detect and respond to security incidents in an organized and methodical manner.

A security incident is defined as a set of events or circumstances involving information technology that may directly or indirectly threaten the confidentiality, integrity or availability of Kount information assets.

All employees must immediately report suspicious events or circumstances to Kount's management, Information Security, or HR, as they feel most comfortable.

For further information, please refer to the Security Management Standard.

Appropriate Segregation of Duties

Kount will maintain appropriate segregation of duties Segregation of duties refers to the use of more than one individual to handle certain important activities to limit risk of unauthorized actions. Examples of this segregation include, but are not limited to:

- Personnel who are responsible for development and testing of code must not also have administrative access to production environments.
- Personnel who submit change control requests must be separate from staff members who approve change control requests.
- Personnel who request access to resources must be separate from staff members who approve and grant access.

Segregation of Production Environment

Segregation of development and production environments is required. Access control mechanisms must be in place to ensure appropriate change control procedures are utilized when modifying code or data. Where practical, development and test environments should exist to provide mechanisms to appropriately manage, plan and test changes prior to implementing in the production environment.

Time Synchronization

Time synchronization services will be employed on systems that contain sensitive information as defined by business, legal or regulatory requirements.

Software Development Policy

All corporate employees and contractors who develop software that is used on the Kount network must follow a Software Development Life Cycle (SDLC).

For more information, refer to Kount's Software Development Standard.

Configuration Management

Kount has various policies related to configuration management which must always be followed. For further details, please refer to the Networking Device Policies and the Change Control Guideline.

Asset Management Policy

Processes, procedures, and tools must be in place for maintaining an inventory of all company assets (Software and hardware). As applicable, the inventory must contain the following attributes.

- Labeling and tracking information
- Lifecycle status and management information
- Role/Functionality
- Make/Model, as appropriate
- Software/Firmware versions, as appropriate

Assets must be validated against inventories and business requirements annually to ensure accuracy of the inventory. Additionally, to ensure unauthorized software is not installed on either production hardware or endpoints, software installation management software and/or FIM shall be utilized.

Access Control Policies

Access Control Policy

Networked systems and devices must employ the use of an access control system that restricts access to users with valid credentials. User access to key computing resources must be granted on a "need-to-know" or least-privilege basis. Administrator, super-user, and other root access privileges must only be granted to administrators within the scope of their job responsibilities.

User Access to Information and User Responsibilities

All systems containing or processing confidential information will utilize the principle of least access for user operations. Two-factor authentication should be used where technically practical and warranted by the value and associated risk of the underlying information asset. Programmatic access via defined API will be the preferred method of database access with direct SQL query capabilities limited to authorized high-level support engineers and database administrators.

Employees are responsible for work performed using their access credentials. Employees must protect all system User IDs, passwords, and other credentials. Individual passwords or access credentials must not be shared with others. Users must never access computer systems using another user's access credentials.

Network Access Policy

Access to trusted and un-trusted networking environments must be controlled. All such interfaces must be approved by Kount Management. For further details, please refer to the Kount the Networking Device Policies.

Session Timeout Policy

Where technically possible, all systems/sessions will be configured to automatically revoke authorization (log out) after fifteen (15) minutes of user inactivity.

Account Provisioning, Termination, and Modification

Access Provisioning

Access will be provisioned based upon predefined, role-based access grants as established in the Logical Access Control Procedure. Requests for additional access beyond what is outlined in the Logical Access Control Procedure must be approved by the CTO or designee in writing. Upon account creation, the user shall be provided with an initial password to login for the first time; upon login this password must be changed.

Access Modification

Similar to provisioning, subsequent modification of access due to changes in job role or responsibility must follow the Logical Access Control Procedure. If requested access does not follow the Logical Access Control Procedure, it must be approved by the CTO or designee in writing.

Access Termination

Procedures must be in place to ensure that User IDs are disabled or removed when users are terminated, transferred, or no longer require access. Management should have the ability to review and archive any critical data even after an account has been suspended, locked out or deleted/removed.

User Authentication and Passwords

All users must have a unique user id allocated for their personal use of company systems. Sharing of passwords associated with unique user ids is prohibited. Backdoors, trap doors and other mechanisms to circumvent authentication are prohibited.

Passwords must be at least 8 characters in length and contain a mixture of numbers, letters and symbols.

Users must change their passwords every ninety (90) days. A new password may not be the same as any of the eight (8) previously used passwords. Functional, group and system accounts for systems not secured with two-factor authentication must have their passwords changed every one hundred and eighty (180) days. User accounts must be automatically locked after five (5) unsuccessful login attempts within a five (5) minute period. Accounts may automatically reset after thirty (30) minutes of inactivity or the user may contact the IT help desk to unlock their account.

If a user forgets their username or password, they must verbally request assistance from the helpdesk. Administrators must verify the user's identity prior to resetting their account. Administrators must not act upon e-mail or telephone requests to reset a user account without conducting additional steps to verify requestor identity.

Accounts that Run Automated Processes

Appropriate controls will be implemented for accounts that provide credentials for automated activities. Those controls may differ from the controls for accounts that provide access for names users. Generally, processes or categories of processes should be run by a unique associated system account.

Application Access Policy

Installation of software on workstations and servers that has not previously been approved, must be approved by the IT Operations and/or Information security team prior to installation.

Powerful System Tools

Use of powerful system tools that could circumvent system and application controls mechanisms must be approved by management. Vulnerabilities that are detected must never be exploited without written consent of management.

Media Handling and Secure Disposal

Storage media should be physically safeguarded during its lifecycle. Information handling and disposal procedures, including those addressing removable media, must be documented. All storage media must be encrypted according to the standards defined in Kount's Data Encryption Standard. Exceptions may be granted for devices used to store non-sensitive information at management’s discretion.

Clear Desk Policy

Confidential client information must always be protected. Employees that create documents containing client confidential information must ensure that information is not improperly shared. Employees should avoid printing documents with confidential client information and must clear their work area of confidential client information when unattended. Documents containing confidential client information should be stored in locked rooms or cabinets.

Secure Disposal and Re-Use of Equipment

Careless disposal or re-use of equipment can cause risks to information confidentiality. Equipment or media must be checked to ensure company data and licensed software have been removed or overwritten before release, re-use, or disposal.

Equipment or media containing sensitive information must be securely wiped in accordance with Kount's Secure Disk Wiping procedure to remove all traces of the information or physically destroyed. However, no information may be destroyed in violation of applicable laws or regulations.

Physical Security

Kount will consistently apply physical security controls appropriate to the information assets located at its facilities. Physical security controls will be based on the value of the information assets contained within the system, the risk associated with the system, and the regulations pertaining to the information assets.

Physical security must be based on the highest valued information asset in the area. For example, rooms containing systems that store information assets of varying sensitivity must be secured to a level appropriate for the most sensitive information asset stored there.

Badge access and visitor log retention in all locations, including corporate offices and co-location data centers, for at least 12 months. Alterations to an employee's badge privileges outside of standard access grants must be requested by a manager or supervisor in writing and approved by the CTO.

For further details, refer to the **Logical Access Control Procedure.**

Video Surveillance

Computer rooms, data centers and other physical areas with systems containing confidential data will be monitored with video cameras. Footage from the cameras will be reviewed as warranted and the data will be preserved for no less than three (3) months.

Physical Access to Network Jacks and Devices

Network jacks (RJ45 or equivalent) located in public areas, such as lobbies, that connect to Kount's internal network will be disabled except during periods of authorized use.

Wireless access points, bridges and gateways are prohibited from connecting to Kount's business networks. A separate guest network may be provided for wireless access.

Identification and Access Badges

Kount issues identification access badges to all employees, temporary employees, contractors and visitors. Employees must not loan their assigned identification access badge to others or facilitate access for others. This includes, but is not limited to, scanning in at a floor or elevator entrance or holding or propping doors open.

If an employee forgets their identification access badge, the receptionist will issue a temporary badge. The receptionist will verify employment status of the individual, notify the employee's supervisor, and request sign in at the log book. At the end of the day, the badge will be returned to the receptionist and the employee will sign out at the log book.

In the event your badge is lost or stolen, please notify the IT help desk and your supervisor immediately so it can be disabled. In case of fire or other emergency, note that badges are not needed to exit the building.

Kount identification & access badges are the property of Kount. Badges must be relinquished upon request to the employee's Supervisor, a member of Kount Management, or a member of Human Resources.

Badge access to secured locations is logged electronically for both successful and unsuccessful access attempts. Logs will be reviewed periodically and retained for a minimum of twelve (12) months.

Visitor Policy

Suppliers, contractors and others conducting business with Kount are hereinafter referred to as visitors. Visitors are subject to Kount's security requirements.

Visitors must sign in at the lobby and provide the name of the employee hosting them at Kount. Upon validating the visit, the receptionist will issue a visitor badge with a visible expiration feature. The host must escort the visitor for the duration of their visit. Visitors requiring access to areas that store, process, or transmit confidential data must obtain authorization from the Operations Team. Upon completion of the visit, the visitor will be escorted to the lobby to return the visitor badge and sign out.

Visitor log records will be reviewed as necessary and retained for a minimum of twelve (12) months.

Periodic Review of User Accounts

Managers must re-certify non-customer user access annually. Each Kount manager is responsible for reviewing the current entitlements for his or her direct organizational reports. The re-certification and reporting process is facilitated by the Information Security team annually in accordance with its annual re-certification procedure.

Privileged Account roles, entitlements, etc. in active director and RSA must be re-certified at least semi-annually by IT Operations.

Logging

Logs Must Be Retained

Fault logging, operational activity logs, and other logs must be retained for regular review or testing. For further detail, consult the Audit Logging Policy.

Monitoring

System Monitoring

System monitoring must be in place to support the availability objectives of the business. Preventative and predictive alerting should be balanced with other availability mechanisms such that the systems provide appropriate access to data.

Auditing

Audit Policy

Appropriate controls and controls will be enabled to accurately audit systems. Audit logs will be available for an appropriate period of time to facilitate forensic investigation.

Acceptable Use

All IT assets and resources are property of Kount and their use must be limited to Company related business in accordance with Company policies and the Employee Handbook.

Company assets and resources may not be used in a way that violates Kount policies. This includes intentionally accessing or transferring non-business-related material that could potentially be defamatory, sexually oriented, pornographic, harassing, threatening, illegal, fraudulent, or offensive in nature.

Additional Guidelines

Some technologies must be strongly controlled due to the related risk. If you are unsure of whether a technology is approved or acceptable, consult the Information Security Team for guidance. See the list below for more information about the acceptable use of some, but not all, technologies

Modems and Emergency Remote Access

Modems, ad-hoc wireless access points and other remote communication technologies represent a significant threat to network security. Unauthorized addition of such devices to the network is strictly prohibited. If such devices are necessary for the proper operation of the company's business, strict policies will be enforced to mitigate the potential risks and diminish opportunities for misuse. For further details, please refer to the Networking Device Policies.

Wireless Connections:

Wireless access points are strongly controlled and limited to authorized devices that require password authentication and conform with Kount's Networking Device Policies. No unauthorized devices may be connected to the network. To obtain authorization consult the Security Team.

Wireless access points within Kount facilities must be logically and/or physically segregated from systems that transmit, process, or store cardholder information. Employees should only use trusted wireless connections with appropriate security measures outside of Kount facilities

Remote Access

Remote access to Kount's networks is provided for business use only and must utilize secure connection technologies, such as a VPN connection. Transfer and/or storage of cardholder data on systems using remote access technologies is strictly prohibited. Data must be protected in accordance with PCI DSS requirements at all times, including when accessing data remotely.

Devices providing remote access capabilities are strongly controlled and limited to authorized devices that conform with Kount's Networking Device Policies.

Personal Devices

No personal devices may be directly connected to internal company networks, including but not limited to Kount's AWS Instances, the corporate network, and cardholder data environment.

Personal devices may access basic business resources available through the public internet, including, but not limited to: email, calendars, approved instant messaging solutions, and SAAS solutions which do not store, transmit or process sensitive data. These devices are subject to the following requirements:

- Jailbroken devices or devices with software installed through unapproved app stores may not access company resources.
- Multifactor authentication must be used to the extent possible
- Devices must use ActiveSync mobile device management enrollment to enforce encryption, passcode requirements, inactivity timeouts, and remote-wipe capability.

- Employees must acknowledge and accept Kount's right to wipe connected personal devices remotely if the device is lost, stolen, or upon termination

Internet and Email Use

Internet access and email are provided for business use. Personal use must be limited in scope and frequency so as not to impact business needs and must not violate any other acceptable use guidelines.

Privacy and Content Filtering

All Non-Public Customer Information (NPCI) must be protected and kept confidential. Examples of NPCI include transaction data, names, addresses, email addresses or other information that could reasonably be used to identify a person or persona that is not available to the general public. Sharing of NPCI with third parties and use of NPCI is restricted by the terms specified in their confidentiality agreement or customer contract. Disclosures of NPCI to third parties must be approved by management prior to the disclosure. Employees and contractors should report any unauthorized disclosures of NPCI to management immediately.

Employees should have no reasonable expectation of privacy, return of information, or access to personal information stored on company-owned devices or services. Workstations capable of external communication shall employ a content filtering solution that protects personal data and rejects or removes any type of executable, batch, script, library, or suspicious attachment from messages. Additionally, workstations shall be secured against accessing websites, services, and protocols considered to be objectionable, insecure, or otherwise not aligned with Kount's objectives.

Third Party Agreement Policy

Business, legal and regulatory requirements related to information security will be included in the negotiation of contracts with third parties.

Non-Compliance

Every member of the workforce at Kount, no matter what their status (employee, contractor, consultant, temporary, volunteer, intern, etc.), must comply with the Kount Information Security policies found in this and related information security documents. Workers who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including termination.

Additional information on compliance and non-compliance with company policy is available through the Human Resources Department.

Exceptions to Policy

Exceptions to this policy will only be granted by an Officer. All approved exceptions must be clearly documented and retained in a secure location. Exceptions will be reviewed by the Security Manager on a regular basis to ensure their continued appropriateness.

Acknowledgement of Policy

Employees will read and acknowledge that they understand the information security policy upon hire and on an annual basis. A sample acknowledgement form is included below:

ACKNOWLEDGEMENT

I acknowledge receipt of the Kount Inc., Information Security Policy, which outlines many of Kount's policies, procedures, and employee responsibilities for information security. I acknowledge that I have thoroughly read and understand the contents of the Information Security Policy and agree to comply with the policies, procedures, and regulations contained therein.

The Information Security Policy is subject to change by management at any time as situations warrant. I understand that changes in the policy will be communicated to me, and I accept responsibility for keeping informed of these changes.

_____

Name Printed

_____

Signature

_____

Date