VERISMIC SOFTWARE

INFORMATION SECURITY POLICY

AUTHOR: Mike Jager, Security & Operations Manager, Verismic Software

1 POLICY PURPOSE & VERSION SUMMARY

Policy Title: Information Security Policy
Responsible Staff: Mike Jager, Security & Operations Officer
Effective Date: September 1, 2017

Recent Major Revision: June 30, 2018
Recent Minor Revision: September 30, 2018
Contact for Additional Information: security@verismic.com

The purpose of this policy is to provide a security framework that will ensure the protection of both corporate and customer Data from unauthorized access, loss or damage. Corporate or customer data may be verbal, digital, and/or hard copy, individually-controlled or shared, standalone or networked, used for administration, research or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately.

2 POLICY AUDIENCE & IMPACTED INDIVIDUALS

The Information Security Policy applies to all Verismic staff, as well as contracting agencies who may be engaged to achieve internal goals or project success. This policy also applies to all other individuals and entities granted access to corporate or customer resources.

3 POLICY DEFINITIONS

Authorization: The function of establishing an individual's privilege levels to access and/or handle data.
Availability: Ensuring that data is ready and suitable for use.
Confidentiality: Ensuring that data is kept in strict privacy.
Integrity: Ensuring the accuracy, completeness, and consistency of data.
Unauthorized Access: Looking up, reviewing, copying, modifying, deleting, analyzing, or handling data without proper authorization and legitimate business need.
Corporate Data: Data that Verismic collects, possesses, or has access to, regardless of its source.

4 DATA MAPPING & CLASSIFICATION LEVELS

Verismic maintains an overall data mapping for both corporate and customer data, however separate unique classification systems for each. This approach allows a more thorough and accurate assessment of data criticality and threat incident likelihood analysis.

Most recently Verismic has optimized data mapping as part of ongoing efforts aligning IT practices with GDPR requirements for customers with European Union data subjects or sources.

Additional information regarding either corporate or customer data classification may be requested by contacting **security@verismic.com.**

5 RESPONSIBILITIES

All Verismic staff, and others granted access to corporate and/or customer data are expected to:

- Understand the data classification levels defined in Verismic data mapping and classification guidelines documented outside this primary information security policy.
- As appropriate, classify the data for which one is responsible accordingly.
- Access data only as needed to meet legitimate business needs.
- Not divulge, copy, release, sell, loan, alter or destroy any Verismic corporate and/or customer data without prior authorization from identified corporate authorities or officers.
- Protect the confidentiality, integrity and availability of corporate and/or customer data in a manner consistent with the data's classification level and type.
- Handle data in accordance with all current and future Verismic information security standards and procedures.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access corporate and/or customer data resources.
- Discard media containing corporate and/or customer data in a manner consistent with the data's classification level, type, and any applicable Verismic stated retention requirement. This includes data contained in any hard copy document (such as a memo or report) or in any electronic, magnetic or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).

6 CORPORATE/CUSTOMER DATA RESOURCE ISOLATION

In many organizations there is at minimum a linkage between internal corporate network systems and customer resources. While security is implemented at the highest level to mitigate uncontrolled to customer resources, the risk is ever-present.

Verismic maintains a strict zero-connection policy between internal corporate systems and customer resources. All customer resources are hosted with Microsoft's Azure, void of internal corporate resources, allowing for complete separation and preventing any uncontrolled access by Verismic staff to both cloud and customer resources.

All access to customer resources hosted within Azure are locked down on several layers outlined throughout this document.

7 CORPORATE/CUSTOMER DATA RESOURCE WHITE LISTING

7.1 Geographic Restrictions

Following resource isolation, Verismic adds another layer of security utilizing geographic region white listing. All technical services staff who require any level of access to corporate and/or customer resources are located at of Verismic's established global offices. This allows a complete denial of access to any region of the world with only a few exceptions, which are then strengthened further with specific Office location IP white listing described in the next section.

7.2 IP Restrictions

As mentioned above, going beyond only geographic white listing, Verismic then restricts access to only IP address matching those global offices containing technical services. With this in place, all access to corporate and/or customer resources must occur from an approved office which in turn provides a strong measure of accountability controlling only authorized staff have physical access to the approved office locations.

8 STRUCTURED TIER-BASED SECURE ACCESS

Access to corporate and customer resources is provided in a traditional structured tiered structure which decreases individual access as the tiers increase.

8.1 Multi-Factor Authentication

Verismic has a mandatory MFA policy in place for all corporate and customer resources which staff are required to perform for access to resources.

8.2 Tier 1 – General Support Staff

For general support of internal and customer issues standard technical services personnel do not require and are not granted access to specific data resources. Break/fix issues require only customer-approved temporary application access for resolution. Once an incident is resolved access for the technical resource is removed.

8.3 Tier 2 – Escalation Server Resource Team

When the need arises for an issue to be escalated it is once again triaged and determined whether the need resides on a corporate or customer resource which is front facing and void of direct data such as web servers, or in rare case a further escalation is required to resolve corporate or customer data issues.

In the event an issue does reside on non-data related resources, an escalation team on average of six individuals will receive escalated support requests, determine the root cause for resolution report back to Tier 1 staff. Tier 2 technical staff cannot access customer data for higher level data related issues.

8.4 Tier 3 – Senior Data & Development Resolution Team

On the rare occasion when direct access to corporate customer data is required for issue resolution, a team of on average three individuals (assigned responsibility/access by local global region) will investigate the escalated issue and if necessarily make corrections to the data anomaly. The result of these efforts is then passed back to Tier 1 technical staff for communication to employee or customer point of contacts.

9 THIRD PARTY PENETRATION TESTING

Verismic on a regular basis engages with leading companies for penetration testing services. While this could be performed by internal staff, Verismic prefers to have the secure state of both resources and product code verified by independent parties.

Areas typically covered during a scheduled penetration test are listed below:

- **Corporate/Product Reconnaissance**
  Passive, Semi-Passive, Active
- **Industry Standard Threat Mapping**
- **Vulnerability Identification**
- **Malicious Input Testing**
- **Application Logic Testing**
- **Platform Exploitation**
- **Post-Exploitation Testing**

10 INFORMATION SECURITY STRUCTURE SUB POLICIES

To provided structure for all objectives within Verismic's Information Security Policy, several structure policies based on recommended PCI compliance standards are implemented. These policies cover a number of disciplines.

All sub items listed in this section are brief overview summaries taken from existing supporting full individual policy documents. Full internal policies are not to be shared with external entities to ensure no sensitive security measures are exposed.

10.1 Acceptable Use

Verismic's employees must protect the company's assets and ensure they are used efficiently and for legitimate business purposes only. Any unauthorized use or distribution of assets is a violation of this policy. Verismic assets include, but are not limited to, intellectual property; strategic, operational, business, and marketing plans; engineering ideas; designs; salary and other compensation information; and all unpublished financial data of Verismic.

10.2 Access Control

Access to information systems shall be controlled based on business and security requirements, and shall only be granted to on a need-to-know basis. Appropriate detective controls shall be implemented to prevent unauthorized access to information systems and network sources.

10.3 Change Control

All major changes to information security management system (ISMS) roles and responsibilities shall follow a standard process that requires a change ticket and approval from ISMS leadership. All changes to network devices, production systems and applications shall be tracked and shall follow a standard process of approval. Verismic may develop a ticket routing system and workflow to ensure that tickets get routed to the appropriate personnel for approval.

10.4 Clear Desk & Screen

Confidential Verismic information stored on physically removable media, including paper and electronic storage devices, shall be locked away unless otherwise required for business function.

All computers and terminals able to access confidential Verismic information must be logged off by the user when left unattended. As an additional control, all computers and terminals shall be protected with a screen and keyboard-locking mechanism when left unattended. The computers and terminals must be locked by a password, token, or similar user-authentication mechanism approved by Information Security.

10.5 Cryptography

Verismic shall use industry-standard encryption technologies in all IT systems that are capable of encryption if those systems are used to process, store or transmit data classified as confidential or privacy data. If Verismic uses encryption and manages keys, the following policies apply. The use of proprietary encryption algorithms is not allowed for any purpose.

Different parts of the world have different national regulations that limit the import/export of cryptographic controls and the trans-border flow of encrypted data. Be aware that government regulations may restrict the import and export of encryption technologies. Verismic's legal team shall understand if the regulation of cryptographic controls is applicable. If applicable, encryption shall be used in compliance with all relevant agreements, laws and regulation.

10.6 Disposal & Destruction

Once no longer required for business need, Verismic Confidential and Privacy Information must be disposed or destroyed in alignment to the acceptable methods defined.

All computer systems, electronic devices and electronic media shall be properly wiped of confidential data before being re-purposed, transferred to another individual, sent out to a vendor for replacement service, or transferred outside of Verismic.

10.7 Human Resources Security

Employees shall sign a contract upon hire that shall state the user and the organization's responsibilities for information security. Employees shall acknowledge through signature that they have read and understand Verismic's policies. Verismic shall ensure that all Verismic employees attend General Security Awareness Training. This may be accomplished by developing, establishing and maintaining a Security Awareness and Training program

10.8 Information Classification

Information assets shall be classified to indicate the need, priorities and degree of protection per the information security risks. All major information assets must be accounted for and have a nominated owner. Information systems that store or process data must be assigned the same classification as the highest classification of data it stores or processes. Classification of data shall be consistent through the organization and follow the classification schema presented in this policy.

10.9 Network and System Security

All Verismic managed network boundary protection devices including, but not limited to fire-walls, routers, network ACLs, and intrusion detection/prevention (IDS/IPS) devices shall provide access to only essential ports, protocols, and/or services to serve Verismic's business needs and to protect against both external and internal threats.

10.10 Operational Security

All critical network components shall have an audit capability to monitor network operation and substantiate investigations of real or perceived violations of network security policies. All information systems running Verismic production application systems that transmit, process, or contain confidential data shall include logs which are reviewed on a regular basis and in real-time as situations demand.

10.11 Physical Security

Physical access shall be granted commensurate with the minimum needed to perform job function.

- Define safety and physical security mechanisms to protect Verismic from natural environmental threats, supply system threats, man-made threats, and politically motivated threats.
- Prevent unauthorized physical access, damage or interference to the Verismic premises and infrastructure, using controls appropriate to the identified risks and the value of the asset(s) protected.
- Place Verismic owned assets and/or assets operated by Verismic that create, process, store, and/or transmit confidential information within a location which minimizes potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Physical security of locations that store media backups containing confidential information will be reviewed at least annually.

10.12 Third Party Management

All contract/relationship owners responsible for services which house, share or provide access to customer information are required to ensure that external parties have entered a formal external party agreement under this procedure and that transitions (of information processing facilities, and any other information assets or personnel) are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.

Contract/relationship owners are responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party. The owners of third-party relationships are responsible for the monitoring and reviewing of the services, reports and records carried out by the third party. The Security & Operations Manager is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.

ABOUT US

Cloud Management Suite allows you to get the complete picture of your entire IT environment from the cloud. Automatically discover network devices, remotely deploy software applications and automate patch management. A single web-based console allows access to any device from anywhere.

Headquartered in Aliso Viejo, California, Cloud Management Suite is a growing and dynamic organization with offices in four countries and 12 partners in nine countries. For more information about Cloud Management Suite and how we've revolutionized IT systems management, visit **www.cloudmanagementsuite.com**.

CALL
US: +1 (949) 270-1903
UK: +44 (0) 1256-806567

CONNECT
www.cloudmanagementsuite.com
info@cloudmanagementsuite.com