TOLLRING

Security Statement for iCall Suite

January 2020

www.tollring.com

Version Control

Document Name:	Security Statement for iCall Suite
Description:	Security Statement for iCall Suite
Document Owner(s)	Cezary Wasilowski
Document Author:	Cezary Wasilowski
Creation Date	17/01/2020
Version number	1.1

Change History

Version	Date	Changed by	Main Changes
Draft	17/01/20	C Wasilowski	Original Document
1.0	17/01/20	A Woollett	Published Document
1.1	10/02/20	S Dhillon / T Martino	Updates to vulnerability management and external libraries/service hosting sections

Introduction

This security statement applies to the products, services, websites and apps offered by Tollring, except where otherwise noted. We refer to those products, services, websites and apps collectively as the “services” in this statement.

Tollring offers call analytics, call recording and fraud management solutions, working closely with partners in order to provide the best quality of service. Tollring values the trust that our customers place in us by letting us act as custodians of their data. We take our responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below.

Compliance

Tollring is compliant with ISO 27001 Information Security Standard and ISO 9001 Quality Management System. Tollring re-certifies those compliances annually. Tollring is compliant and follows the General Data Protection Regulation (GDPR).

Service Hosting

When delivered as an ‘Over-The-Top’ Service, all servers, applications, network and data is hosted in the Microsoft Azure Public Cloud. For European Service Provider partners, these services are held in Azure West Europe (Netherlands) Data Centre. For Service Provider Partners operating in the United Kingdom, the service is hosted in Azure UK South Data Centre. For this deployment method, an on-site recording server is also deployed in the Service Provider’s data centre. For services delivered fully in the Service Provider’s Data Centres, all servers, applications, network and data is fully hosted by the Service Provider.

Access Control

Access to Tollring technology resources is only permitted through secure connectivity (VPN) and requires authentication. Our password policy requires complexity, expiration and lockout. Access to the resources is restricted and closely monitored. Access is granted only for the period necessary to perform administrative or technical support tasks and is revoked after tasks are completed. All permissions are reviewed quarterly.

Security Policies

Tollring maintains and regularly reviews and updates its security policies on at least an annual basis. Employees must acknowledge policies on an annual basis and undergo additional training if required. The training schedule is designed to adhere to all specifications and regulations that are applicable.

Personnel

Tollring communicates its information security policies to all personnel (who must acknowledge this) and requires new employees to complete a full induction process, as well as providing ongoing privacy and security training.

Dedicated Security Personnel

Tollring has a dedicated security and compliance department, which focuses on application, network, and system security. This team is also responsible for security compliance, education, and incident response.

Vulnerability Management and Penetration Tests

Tollring maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third party vendors. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Approach for Penetration Testing

OWASP Top 10 methodology will be used for testing the application.

We shall also perform a penetration test to stimulate a number of scenarios such as:

- Assess the application to ensure a robust security posture.
- Stimulate the penetration test from an attacker point of view to gain access to the application data in an unauthorised manner.
- Users with authentication credentials trying to gain unauthorised access to other client data or account information.

All of the tests will be carried out only on Pre-Production/Test environments only.

External Libraries

All third-party library versions are checked for known vulnerabilities and remedial actions are taken.

All third-party libraries are checked for commercial use and licenses.

Encryption

All data in transit is encrypted using secure TLS cryptographic protocols. Data is also encrypted at rest.

Development

Our development team employs secure coding techniques and best practices. Development, testing, and production environments are separated. All changes are peer-reviewed and logged for performance, audit, and forensic purposes prior to deployment into the production environment.

Asset Management

Tollring maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software.

Information Security Incident Management

Tollring maintains security incident response policies and procedures covering initial response, investigation, customer notification, public communication, and remediation. These policies are reviewed regularly and tested annually.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. However, if Tollring learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under GDPR regulations, as well as any industry rules or standards applicable to us. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers with all information necessary for them to meet their own regulatory reporting obligations.

Business Continuity

Tollring infrastructure is backed up daily. Backups are encrypted and stored within the production environments to preserve their confidentiality and integrity and they are tested regularly to ensure availability.

Logging and Monitoring

All logs from applications and infrastructure systems undergo analysis by authorised Tollrign personnel. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.