HRACUITY®

HR Acuity Security Overview

At HR Acuity, we take the security of our client data seriously. The purpose of this document it to be transparent with our clients about the security provisions we have in place to protect your confidential information. Following you will find answers to the questions we are most commonly asked. Accompanying documents are also available for your review within the HR Acuity Information Security Portal and updated as required.

Solution Overview

HR Acuity is a SaaS-based employee relations technology solution used by organizations to achieve consistency in the way they track, investigate, and analyze employee issues.

Our solution was developed using the Microsoft software stack and adheres to the Microsoft.Net MVC pattern-based framework that enables a clean separation of concerns and provides full control for creating sophisticated features that use the latest web standards.

Certifications

HR Acuity has received its SOC 2 Type 1 Certification, and is on track to receive SOC 2 Type 2 certification in early 2019. We are also certified with the EU-US Data Privacy Shield. We have chosen to partner with Microsoft Azure for cloud storage in their Tier IV data centers. Microsoft Azure is SOC 2 Type 2 Certified. Certificate and Audit reports are available within the HR Acuity Information Security Portal.

Security Oversight

To ensure the protection of client data, we have a formal Information Security and Risk Program in place. As part of that program, our information security and risk management team ensures security and privacy policies align with industry standards, conducts yearly Information Security Policy reviews, and manages our Security Incident Response program. In addition, all third-party vendors are contractually obligated and annually reviewed to ensure they comply with the HR Acuity security standards.

The HR Acuity leadership is charged with ensuring all HR Acuity employees are knowledgeable and following best practice protocols for managing data and security. High priority is given to effective security awareness and training throughout the organization. This includes implementing a viable information security program comprised of a strong awareness and training component. The CTO, in cooperation with the senior HR Acuity leadership team, is ultimately responsible for the security of data and assets of HR Acuity and ensuring that a consistent, well-supported and effective security program is implemented and maintained.

Data Centers

HR Acuity partners with MS Azure Cloud Infrastructure managed and operated by Microsoft. Currently, HR Acuity leverages datacenters in South-Central and North-Central United States. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff 24/7/365.

The HR Acuity solution is managed/ deployed on the Microsoft Azure ASE environment and is isolated and protected using Web application firewall (WAF) and Network security group (NSG) with restricted inbound/ outbound rules.

Database Security

Database security includes Transparent Data Encryption algorithm (TDE), Dynamic Data Masking (DDM), and Advanced Threat Protection (ATP).

- Transparent Data Encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, Azure Data Warehouse, and Azure BLOB Storage against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, BLOB Storage and transaction log files at rest using AES 256-bit algorithm. The encryption uses a database encryption key (DEK), protected by a build in server certificate. The built-in server certificate is unique for each server and is rotated every 90 days.

- Dynamic Data Masking (DDM) limits sensitive data exposure by masking it to non-privileged users.

- Advanced Threat Protection (ATP) is a cloud-based security solution that identifies, detects, and helps investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP enables SecOp analysts and security professionals to detect advanced attacks in environments to:

    - Monitor users, entity behavior, and activities with learning-based analytics

    - Protect user identities and credentials

    - Identify and investigate suspicious user activities and advanced attacks throughout the kill chain.

    - Provide clear incident information on a simple timeline for fast triage

User Authentication

HR Acuity offers SSO authentication, IP Filtering, role-based access control (RBAC), and multi-factor authentication (MFA) as part of user authentication and authorization services. SSO is modeled on industry best practices and frameworks such as ISO 27001 and NIST 800-53. SSO communications are encrypted and transmitted over TLS 1.2.

Passwords are encrypted using Bcrypt Hash Algorithm based on Blowfish Cipher. Enforcement of our password policy ensures that passwords are between 9–20 characters in length, include at least one number, one upper case letter, one lower case letter and one special character. Password cannot contain more than two repetitive characters one after another (e.g. 'aaa' or '555').

Vulnerability Management

HR Acuity uses Qualys and Burp Suite for internally testing any software runtime vulnerabilities on at least a quarterly basis. We also employ IBM SAST and DAST tool to identify any cybersecurity threats or vulnerabilities every month.

External penetration testing is performed by an independent third-party firm at least once a year or with any major release – whichever is sooner.

HR Acuity has a dedicated team and Security Operations Center (SOC) that actively monitors all of our resources to identify potential security incidents 24x7x365. HR Acuity has implemented WAF and SIEM solutions to monitor/ secure all web traffic.

Secure Software Development

HR Acuity embeds security controls in our S-SDLC process to ensure security throughout the development process and provides resources for security assessment, testing and review.

- Manual code reviews are done before any code merge to the Master branch.
- Static Analysis Security Analysis (SAST) is performed using IBM App Scan during the development process to identify and remediate any security vulnerabilities before production release.
- Dynamic Analysis Security Analysis (DAST) is performed on the runtime environment to find any OWASP 3.0 related vulnerabilities on a monthly basis.
- Targeted manual security testing is performed by product security engineers based on the highest identified risks in security risk assessment
- At least annually, HR Acuity engages with a third-party world class application security firm to perform automated and manual penetration testing and dynamic analysis.
- Continuous assessment of global security and compliance across web applications and cloud infrastructure is managed using Qualys vulnerability management solution.
- To ensure ongoing security awareness, HR Acuity security engineers meet regularly to share knowledge on emerging trends and threats and to evangelize best practices and raise overall awareness related to site security throughout the organization.

Patch Management

OS and runtime patches are managed by MS Azure patch policy. These patches are updated monthly and follows MS Patch Tuesday Schedule. Severe vulnerabilities that require immediate patching, such as zero-day vulnerabilities, and/or high-priority security updates are handled on a case-by-case basis.

Servers managed by HR Acuity must have and maintain up-to-date operating system (O/S) patches. A systems patch cycle for all server O/S is scheduled once per month (3rd Saturday of every month), with no more than thirty (30) days between patch updates. All other patching is applied based on the Common Vulnerabilities and Exposures (CVE): Ratings with High and critical severity are handled on a case by case basis; and all others within thirty (30) calendar days.

Data Management & Protection

HR Acuity's software provides appropriate controls to ensure data integrity. Customer data is segregated logically using combination of primary/unique keys. SFTP is used to import/export data from customers, with encryption using SSH key and pgp/gpg keys.

Access to HR Acuity information systems is only provided to Database Administrators. Multi-factor authentication is enforced to access any information system asset.

Any data access required by HR Acuity to support the Client/User needs is only available with client pre-authorization on a per incident basis. User roles and access are reviewed at least every 3 months. No client data is ever stored in Hard Copy and portable electronic media ports are disabled on our systems to protect against improper downloads.

Data Backup, Recovery & Response

We have a fully tested and functional DR Infrastructure focused on uptime, accuracy, failover, high availability, data redundancy, and backups. Geo-replication of our databases is in place within different geographic regions within the continental United States.

- The complete data set is backed up once a day with incremental backups completed every 5 minutes.
- Recovery Point Objectives (RPO) for the system containing client data is every 5 minutes. HR Acuity Primary and DR databases are in sync at all times.
- Recovery Time Objectives (RTO) for HR Acuity's application is instantaneous. In the instance primary servers are unavailable, traffic is auto routed to DR/Secondary servers.
- HR Acuity also has a documented and communicated incident response program that is managed by the Information Security and Risk Management Team.
- Both the incident response and disaster recovery programs are tested no less than annually.

Personnel Management

Background screening checks are required for all employees and contractors. In addition, employees/contractors must sign an NDA document and are restricted with strict permission/roles. Access permissions are reviewed on a regular basis. Security training and assessment – including social engineering - occurs on an ongoing basis for all HR Acuity employees.

Version Management

Version	Revisions Made	Approval	Date
1.0	Initial draft and review	D. Muller	12/31/18
1.1	Updated SSO		