HRACUITY®

HR ACUITY INFORMATION SECURITY PROGRAM

CONFIDENTIAL (for internal use only)

www.hracuity.com

Table of Contents

I. Purpose and Scope

HR Acuity is committed to high standards of excellence for protection of information assets and information technology resources that support the HR Acuity On-Demand environment ("HRAOD"). HRAOD processes, stores, and transmits electronic information to conduct its business functions. Without the implementation of appropriate controls and security measures, these assets would be subject to potential damage or compromise to confidentiality or privacy, and the activities of HR Acuity and its clients are subject to interruption. (Ref: ISO/IEC 27001:2013)

The purpose of the Information Security Policy is to set forth the underlying tenets, framework, and reasoning for the HR Acuity Information Security Management System (ISMS) in accord with the requirements of ISO standard ISO/IEC 27001:2013. The purpose of the HR Acuity ISMS is to establish guidelines for achieving appropriate protection of HR Acuity electronic information resources and to identify roles and responsibilities at all levels

The provisions in the Program apply to all information subjects and objects that have access to or function in HRAOD. Some entities may be subject to additional federal, state, international law or other regulations.

II. Definitions

The following terms used in this Program are defined in Appendix A:

Authorized Individual

Data Custodian

Data Owner

Electronic Information Resource (Resource)

Encryption

Essential Resource

Restricted Data

Restricted Resource

Team Member

III. Information Security Program Overview

A. Roles and Responsibilities

To ensure, to the extent possible, the confidentiality, integrity, and availability of HR Acuity information assets, HR Acuity has identified Vikas Gupta, CTO, to perform the function of Information Security Officer (ISO) along with Lawrence Brown, Chief Information Security Officer (CISO) with responsibility for the Program. The ISO will be responsible for the implementation of the Program and periodic evaluation of the Program to ensure that the Program adequately addresses operational or environmental changes.

Responsibility for compliance with the Program will rest with a number of individuals, and the ISO must facilitate this compliance through collaborative relationships within HR Acuity and with its clients and trusted third parties.

All Team Members of the HR Acuity organization are expected to comply with the policies and procedures and to exercise responsibility appropriate to their position and delegated authorities.

All procedures within this Program will be practiced in accordance with HR Acuity Human Resources policies and guidelines.

B. Program Objectives

The overall security objectives of the Program are to ensure confidentiality, integrity, and availability regarding IT security. These objectives are the paramount goals for ensuring the protection of information and Resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

> *Confidentiality*: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure.
>
> *Integrity*: guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. The level of impact of unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a Resource.
>
> *Availability*: ensuring timely and reliable access to and use of information. Emergency management planning must take into account the availability requirements of a particular Resource to determine its inclusion in emergency and disaster recovery planning.

The Program components include:

- Risk assessment strategies to identify vulnerabilities and threats to information resources
- A security plan that includes recommendations for administrative, technical, and physical security measures to address identified risks relative to their sensitivity or criticality,
- Incident response planning and notification procedures,
- Guidelines for security awareness training and education as appropriate for the HRAOD environment
- Appropriate review of third-party agreements for compliance with federal, state and international laws and compliance requirements.

C. Risk Assessment

The HR Acuity ISMS Risk Management process is designed in accord with the methodology described in the standard ISO/IEC 27001:2013 Information Technology-Security Techniques-Information Security Risk Management and will be performed on at least an annual basis.

- Provide an inventory of and the nature of electronic information resources,
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources, and
- Identify the level of security necessary for the protection of the resources.

This risk assessment will:

- Take into account and prioritize the potential adverse impact on HR Acuity's reputation, operations, and assets,
- Ensure full review and classification of HR Acuity information assets by the level of security objectives assigned to them,
- Be conducted by qualified personnel,
- Address the appropriateness and frequency of staff and management security awareness training.

After completing the annual risk assessment, an information security plan will be developed to take into consideration the acceptable level of risk for systems and processes. Appropriate mechanisms to safeguard information will be selected relative to the *security objectives* determined by the risk assessment. Controls selected to mitigate risks will include administrative, operational, technical, physical and environmental measures as appropriate. The information security plan will identify cost-effective strategies to be implemented consistent with organizational goals and functions for mitigating that risk. The security plan will account for the management, use, and protection of information that has some level of confidentiality, and identify the procedures and controls that will be implemented to enhance security for information assets.

D. Governance

The purpose of this Information Security Governance Plan is to set forth the organization and responsibilities within the HR Acuity Information Security Management System (ISMS), in accord with the requirements of ISO Standard ISO/IEC 27001:2013.

E. Classification of Information

All HR Acuity information is categorized into four main classifications:

- HR Acuity Public
- HR Acuity Confidential
- HR Acuity Third Party Confidential
- HR Acuity Third Party Sensitive

HR Acuity Public information is information that has been declared public knowledge by someone with the authority to do so and can freely be given to anyone without any possible damage to HR Acuity or its clients.

HR Acuity Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in HR Acuity Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of HR Acuity Confidential information is *HR Acuity Third Party Confidential* information. This is confidential information belonging or pertaining to another corporation, in particular our clients, which has been entrusted to HR Acuity by that client under non-disclosure agreements and other contracts. HR Acuity Third Party Confidential may also include *HR Acuity Third Party Sensitive* meaning any information that identifies or can be used to identify an individual, including information related to a third party and its affiliated clients' personnel (e.g., employees, temporary workers and independent contractors), clients, suppliers and invitees, that is provided to, or obtained, used, accessed, maintained, or otherwise handled by, HR Acuity in connection with providing our services to our clients.

Information classified as HR Acuity Third Party Sensitive is considered *Restricted Data*. For the purpose of the ISP and the practices laid out in this program, “Highly Confidential Information” will refer to all Restricted Data as well as HR Acuity Third Party Confidential Information and HR Acuity Confidential Information including but not limited information containing trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.

In order to protect the proliferation of Restricted Data, the following policies are in place:

- Restricted Data should not be transferred to another individual or system without approval of the Data Owner. Before Restricted Data is transferred to a destination system, the Data Owner must follow established procedures to ensure that Authorized Individuals implement appropriate security measures.

- Data Owners for Restricted Data should ensure that Authorized Individuals are informed of this constraint when access is originally requested. The Data Owner may choose to require the Authorized Individual's signature to document approval of release of restricted data.

- Security measures on destination systems should be commensurate with security measures on the originating system.

- Data Owners should ensure that HR Acuity Third Party Sensitive data is not unknowingly transferred during a migration and that the proper controls are in place to safeguard that data. HR Acuity will issue a notice to clients advising them not to store government identifiers such as Social Security number, Taxpayer Identification Number, passport number, driver’s license number or other government-issued identification number, insurance policy number or financial account number, such as a credit card or debit card number, or bank card information, with or without any code or password that would permit access to the account, or signature in HRAOD.

All client service agreements include requirements regarding retention or disposition of data after the Restricted Data is no longer needed on the destination system.

IV. Administrative Controls

All employees or third party contractors/vendors working with Restricted Data are expected to employ security practices as appropriate to their responsibilities and roles, which include, but are not limited to:

- Taking appropriate actions to ensure the preservation of data confidentiality and integrity,

- Taking appropriate precautions to ensure protection of data from unauthorized access, modification, or destruction,

- Complying with license agreements, terms and conditions, and laws pertaining to intellectual property, and

- Complying with identified security procedures.

A. Authorized Access

Access to all Restricted Data will be granted in a controlled manner based on need to know and subject to the approval of the designated information Data Owner. Team Members will be explicitly granted access to Restricted Data; there is no implicit right of access. Controls have been developed, implemented, monitored and maintained to create accountability and to prevent any compromise of the confidentiality, availability, and integrity of information assets.

In order to ensure authorized access to all employees or third-party contractors or vendors working with Restricted Data, the following procedures to have been put in place:

- As part of the hiring process and before receiving access to Restricted Data, Team Members must undergo background checks performed to include criminal checks and verification of employment records.

- Any Team Member with access to Restricted Data will also undergo drug screening as a condition of employment.

- Authorized access, both logical and physical, shall only be granted to those Team Members who have a legitimate business reason to access specific Resources (Authorized Individuals).

- Upon hire, a new Team Member’s Supervisor will review and propose access. Data Owner must approve in writing any request for authorization and assignment of the associated level of privilege. Records of this approval will be retained. Data Owners must not approve their own access.

- Team Members must sign the HR Acuity Security Policies Acknowledgement prior to being granted access to HR Highly Confidential Information and reconfirm on an annual basis.

- Access for Team Members who change roles or transfer to other areas of HR Acuity should be immediately given the access required for the new role. Access that is no longer required for the new role should be removed or disabled immediately.

- When access is granted, Team Members are responsible for all system activity under their unique account and have the responsibility to protect their account by creating and maintaining passwords compliant with the HR Acuity Acceptable Use Policy. In addition, Team Members are responsible for maintaining the confidentiality of their unique ID and password by not sharing it with any other party.

- HR Acuity will re-evaluate the privileges granted to users annually to ascertain that the access is still commensurate with the user's job responsibilities. User accounts found to be invalid should be disabled.

- Non-employee user accounts and access privileges, including third parties, contractors, consultants, and temporaries, shall be re-evaluated every six months. User accounts found to be invalid should be disabled.

- In the event of disciplinary action where there is a concern that access to Resources endangers the integrity of such Resources, management will review and act to restrict, suspend or terminate access.

- Upon termination or when job duties no longer require a legitimate business reason for access, all access will be revoked. Further for Team Members who announce their decision to terminate, access may be removed if continued access may result in an unacceptable level of risk. Access shall be revoked for individuals on a leave of absence.

- Upon termination, Supervisor will ensure disposition of electronic information resources.

- During any extended leave of absence, access privileges should be revoked or restricted, as appropriate.

B. Acceptable Use

In order to ensure acceptable usage of critical technologies, all employees, contractors, consultants, temporary and other workers at HR Acuity, including all personnel affiliated with third parties must adhere to the HR Acuity Acceptable Use Policy. This policy applies to information assets owned or leased by HR Acuity, or to devices that connect to a HR Acuity network or reside at a HR Acuity site such as personal mobile devices used to access HR Acuity information or network.

C. Code of Conduct

The success of HR Acuity is dependent on the trust and confidence we earn from our employees and customers. We gain credibility by adhering to our commitments, displaying honesty and integrity, and reaching company goals solely through honorable conduct. It is easy to *say* what we must do, but the proof is in our *actions*. Ultimately, we will be judged on what we do. As such all HR Acuity employees must adhere to our Code of Conduct Policy which centers around the following principles:

- **Our Values:** The HR Acuity company values are exactly the same as those in which we help our clients achieve by using our services **Respect. Fairness. Transparency.**

- **Respect for the Individual:** We all deserve to work in an environment where we are treated with dignity and respect. HR Acuity is committed to creating such an environment because it brings out the full potential in each of us, which in turn contributes directly to our, and our customer's, success. We cannot afford to let anyone's talents go to waste

- **Create a Culture of Open & Honest Communication:** At HR Acuity, everyone should feel comfortable to speak his or her mind, particularly with respect to ethics concerns. Managers have a responsibility to create an open and supportive environment where employees feel comfortable raising such questions. We all benefit tremendously when employees exercise their power to prevent mistakes or wrongdoing by asking the right questions at the right times. HR Acuity will investigate all reported instances of questionable or unethical behavior. In every instance where improper behavior is found to have occurred, the company will take appropriate action. We will not tolerate retaliation against employees who raise genuine ethics concerns in good faith.

- **Set the Tone at the Top:** Management has the added responsibility for demonstrating, through their actions, the importance of this Code. In any business, ethical behavior does not simply happen; it is the product of clear and direct communication of behavioral expectations, modeled from the top and demonstrated by example.

HR Acuity is an equal employment/affirmative action employer and is committed to providing a workplace that is free of discrimination of all types, including abusive, offensive or harassing behavior.

To make our Code work, managers must be responsible for promptly addressing the ethical questions or concerns raised by employees and for taking the appropriate steps to deal with such issues. Any employee who feels harassed or discriminated against should report the incident to his or her manager or to human resources.

Managers should not consider employees' ethics concerns as threats or challenges to their authority, but rather as encouraged form of business communication. At HR Acuity, we want the ethics dialogue to become a natural part of daily work.

Employees are encouraged, in the first instance, to address such issues with their manager or human resources, as most problems can be resolved quickly. If for any reason that is not possible, or if an employee is not comfortable raising the issue with their manager or HR, HR Acuity's CEO operates with an open-door policy.

D. Violations

In order to ensure compliance with the above requirements, the following procedures have been put in place:

- Supervisors and department heads are responsible for promptly reporting any known or suspected policy violations of the provisions in this policy to the Data Owner or Custodian.
- Team Members who become aware of the occurrence of any violation should report the violation promptly to their supervisor, department head. Data Owners or Custodians should be notified of such violations in accordance with departmental procedures.
- Data Owners may withdraw the privileges of any individuals who violate these policies if, in their opinion, continuation of such privileges threatens the security (confidentiality, integrity, and availability) of restricted or Essential Resources.
- Depending on the nature of the violation and the likelihood of a recurrence, the Data Owner or Custodian shall take prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation occurred.
- In the event of a violation of the provisions in this policy that involves possible unlawful action by an individual, the employee's immediate supervisor, or other appropriate official should immediately be notified. Notification should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence.
- HR Acuity reserves the right to revoke access to any Resource for any individual who violates the provisions of this policy

V. Identity and Access Management

HR Acuity access control measures include secure and accountable means of *authorization* and *authentication*.

Authorization is the process of determining whether or not an identified individual or class has been granted access rights to an information resource and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

Authentication is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

A. Access Controls

Access controls are put in place to restrict Resource access to Authorized Individuals. Such mechanisms will be implemented to ensure that security objectives are in compliance with federal, state and international law. This includes not only the primary operational copy of the information, but also data extracts and backup copies. Authorized Individuals and their specific level of privilege should be specified by the Data Owner, unless otherwise defined by HR Acuity policy.

In order to ensure compliance with the above requirements, access controls in place for HR Acuity consist of but are not limited to:

- GIT is used for access control with different branches (Development, QA, UAT, Production) which can only be accessed by Authorized Individuals with login credentials. Access to each branch is limited to ensure checks and balances. For example, developers have access to only development branch whereas Team Lead and Development Manager have the access to the UAT and Production branches.
- Remote access is allowed based on IP address access control list.
- Certificate based access control available for web application only
- Records of access events are to be maintained consistent with audit log guidelines

Rights of access to modify data are to be performed according to procedures that ensure data integrity. Exceptions may be made on a case-by-case basis but should always be performed in a controlled manner and with the knowledge of the Data Owner

B. Password Authentications

The following procedures have been put in place to ensure appropriate authentication permissions are in use:

- Supervisors and department heads are responsible for promptly reporting any known or suspected policy violations of the provisions in this policy to the Data Owner or Custodian.

- Passwords selected by individuals or automatically generated to protect access to information resources should be difficult to ascertain and should comply with HR Acuity password standards.

- Passwords to individual accounts should never be shared with other individuals unless specifically approved and documented as an exception to policy by Data Owners responsible for the Resources to be accessed.

- HR Acuity Password Standards: Passwords must be a minimum of 9 characters and contain at least one alphabetic, one numeric, and one special character.

- Passwords must be changed regularly. The change interval should not exceed 90 days.

- Passwords must not be inserted into email messages or other forms of electronic communication unless protected.

C. Session protection

In order to ensure compliance with technical security mechanisms to prohibit and minimize the risk of unauthorized access to Resources by others who might gain control of the working session, the following procedures have been put in place:

- Sessions should be set to timeout automatically after 30 minutes of inactivity

- Applications in HRAOD should be set to timeout after 30 minutes of inactivity

D. Privileged Accounts

Privileged Accounts are especially sensitive. As such, HR Acuity has established procedures, commensurate with the level of risk involved, to ensure that abuse will not occur.

- Team members assigned Privileged Accounts are fully informed regarding appropriate access and disclosure of information. An annual agreement shall be reviewed, signed and filed, by all team members with access to privileged accounts at time of hire, time of access to these accounts (if post-hire date) and annually. This agreement will fully inform the team member that that Privileged Accounts should not be used to seek out personal or confidential information relating to others, or to disclose or otherwise use what they may have observed, either incidentally or resulting from authorized monitoring conducted.

- The number of Privileged Accounts should be kept to a minimum, and only provided to those personnel whose job duties require them.

- Personnel who require Privileged Accounts should also have non-privileged accounts to use when not performing system administration tasks and should be instructed not to use their Privileged Accounts for non-authorized purposes.

- Activities performed using a Privileged Accounts should be logged, where feasible, and the logs should be reviewed on a regular basis by an independent and knowledgeable person.

- Use of Privileged Accounts should be monitored periodically to ensure they are being used for authorized purposes.

VI. Systems and Application Security

A. Systems Personnel

- HR Acuity designated Team Members who manage, operate, and support HR Acuity system and application security ("Systems Personnel"), are expected to follow all applicable HR Acuity policies, and use appropriate professional practices in providing for the security of the systems they manage.

- In addition to periodic risk assessments, Systems Personnel will routinely evaluate Resource exposure to potential and known threats and deploy controls commensurate with the level of risk and magnitude of the harm that could result from loss, misuse, or unauthorized access to supported systems, applications, and data.

- The principle of separation of duties will be employed to ensure that responsibilities for critical functions are divided among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such controls keep a single individual from subverting a critical process.

B. Backup and retention

The following procedures shall be in place to ensure the routine backup of the HR Acuity applications and data:

- Backup of the Web app, Blob storage and Database is automated.

- For Web app, backup is scheduled weekly.

- For Blob storage and database, backup is scheduled for daily.

- The backup files are stored in the Blob storage account. Backed up folder can be accessed only by System Personnel.

- All data is automatically encrypted prior to persisting to storage and decrypts prior to retrieval.

- Backup will be retained for 30 days.

All backup and other retention services for data will comply with HR Acuity policies regarding data retention.

C. System protection

HR Acuity deploys the following procedures to ensure that host *Restricted* or *Essential Resource*s and systems are protected from "malicious software."

- HR Acuity Azure Web portal and VM's are enabled with Microsoft Antimalware, real-time protection capability that help identify and remove viruses, spyware, and other malicious software and unwanted software attempts to install itself or run on our systems.

- 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 on applications, networks, infrastructure, software and other technologies used in connection with the protection of the Client Data.

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

- Activities are monitored and controlled on a regular basis.

D. Patch management

In conformance with change management processes (see Section VIII) and HR Acuity minimum standards (see Section XIV), Systems Personnel will in a timely manner, update versions of the operating system and application software for which security patches are made available. In general, such security patches should be applied within 30 days of release by vendor.

E. Software Development

Development and maintenance of any systems, whether performed by HR Acuity personnel or performed by any vendor engaged by HR Acuity personnel, should conform to the specifications of HR Acuity S-SDLC. Application development and maintenance efforts should also conform to any local standards, procedures, guidelines and conventions.

In order to ensure compliance with the above requirements, the following procedures have been put in place:

- Developers should conduct a privacy impact assessment, i.e., an analysis of how personal information should be collected, stored, shared, and managed for any application that will be used to process personal information. Examples of personal information would be: cardholder data, SSN, etc. (Ref: ISO/IEC 27001:2013) The privacy impact assessment should also consider whether any application or software component will require European Union (EU) Data Protection. EU Data Protection will be handled on a case by case basis and its requirements listed in the privacy impact assessment.

- Configuration standards will be promulgated for each operating system and networking component. Examples of acceptable standards may be found from NIST or SANS

- Databases which store Restricted Data must be hosted on an internal segment separated from the DMZ

- Each server should have only one primary function.

- File Integrity software will be used to ensure the integrity of critical system files.

- 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.

- Network Vulnerability Security Tests are conducted internally on a monthly basis.

- Targeted manual security testing is performed by product security engineers based on the highest identified risks in security risk assessment.

- Continuous assessment of global security and compliance across web applications and cloud infrastructure is managed using external 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.

VII. Network Security

In order to protect the network from Denial of Service attacks, malicious code, or other traffic that threatens the network, the following procedures are in place:

- Firewall rule sets are checked on a quarterly basis

- Firewall accesses are be logged and checked on a regular basis
- Firewalls are set by default to “deny any/any”
- All Internet connections as well as connections to and from a demilitarized zone are firewalled from the internal HR Acuity network.
- Only protocols with a justifiable business need may be allowed through the firewall.l
- Allowed protocols are documented and approved by the Data Custodian.
- Firewall configuration changes must be approved through a change control process.
- A current network diagram of the HR Acuity network is maintained and updated on an annual basis.
- All networks which store, process, or transmit “Restricted” data must be documented.
- No wireless networks are allowed to connect to the HR Acuity environment.
- No direct access is allowed from the Internet to the HR Acuity environment.
- Default accounts and passwords for all operating systems, network devices and applications are changed to meet the requirements of the Identity Management standard.
- HR Acuity environment will undergo an annual penetration test.
- Firewall and router configurations will be reviewed every 6 months.

VIII. Change Management

Changes to any *Restricted* or *Essential Resource* will be performed in compliance with the following HR Acuity Change Management procedures:

- monitoring and logging of all changes,
- steps to detect unauthorized changes,
- confirmation of testing,
- authorization for moving application programs to production,
- tracking movement of hardware and other infrastructure components,

- periodic review of logs,
- back out plans, and
- user training.

A. Audit Logs

HR Acuity audit logs will be managed in a manner that facilitates these benefits while protecting the confidentiality and integrity of the information contained in these logs. In particular, the log management infrastructure will capture information to aid analysis about access, change monitoring, malfunction, resource utilization, security events, and user activity.

In order to ensure the availability of logs, the following procedures have been put in place:

- Audit logs will be backed up to a centralized server and reviewed on a daily basis.
- File integrity software will be used to ensure audit logs are not tampered with.
- Audit logs will be retained for a minimum of one year.
- The following are the logs maintained:
    - Application Log
    - Web Server Log
    - System Log
    - Security Log
    - Audit Log
    - Network Log

IX. Encryption

Suitably strong encryption measures shall be employed and implemented for information in storage and during transmission using following encryption procedures:

Transit - - Restricted Information shall be encrypted during transmission using measures strong enough to minimize the risk of the information's exposure if intercepted or misrouted for example HTTPS and Transport Layer Security.

Storage - Application data shall be stored with encryption at rest. Encryption shall be performed at the database level and storage level.

Restricted Information may not be retained on portable equipment.

Key management - HR Acuity shall implement encryption key management plans to ensure the availability of encrypted authoritative information.

- The encryption key management plan shall ensure that data can be decrypted when access to data is necessary. This requires key backup or other strategies to enable decryption, thereby ensuring that data can be recovered in the event of loss or unavailability of cryptographic keys.

- The encryption key management plan shall address handling compromise or suspected compromise of encryption keys. In addition, the plan should address the impact of a key compromise on system software, hardware, other cryptographic keys, or encrypted information.

- The encryption key management plan shall include a process to determine whether any encryption keys may have been compromised as a result of any security incident.

- The encryption key management plan shall include periodic review to ensure suitably strong encryption.

- Users shall be made aware of their unique role if they are given responsibility for maintaining control of cryptographic keys.

- Background checks shall be conducted for HR Acuity employees who control and manage encryption keys and key management software and hardware.

X. Physical and Environmental Controls

A. Physical Access Controls

Controls for limiting physical access to facilities housing *Restricted* or *Essential Resource*s should be implemented through the use of combination locks, key locks, badge readers, manual sign in/out logs, verification of identification, etc. The ability to track both ingress and egress of all individuals should be maintained as appropriate.

Limiting physical access to facilities may also include technical mechanisms, such as use of proximity card readers. In those instances, technical access control guidelines apply.

Records of access events should be maintained consistent with audit log requirements.

Entry to a data center must be able to be tracked to an individual with at least the following information:

- Name
- Time entered
- Time exited

Monitoring cameras shall be in place inside the physical data center.

B. Tracking Reassignment or Movement of Devices and Stock Inventories

Procedures should be implemented that:

- track the receipt, reuse, and removal of hardware and electronic media, including documentation of hardware reassignment. Removal of *restricted* or other sensitive information should be conducted in accordance with procedures below regarding final disposition of equipment.
- maintain records documenting repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks.

C. Disposition of Equipment

Procedures are in place to ensure implementation of controls to address the re-assignment or final disposition of hardware and electronic media, including requirements that ensure complete removal of *restricted* or other sensitive information as appropriate, such as by shredding, overwriting a disk, or employing professional data destruction services as commensurate with risk. Sufficiently strong disk encryption may be used as an alternative mitigation. If electronic media or hardware is subject to a litigation hold, final disposition of these resources must be conducted in such a manner that ensures that relevant data is not lost,

D. Portable Devices and Media

With the exception of HR Acuity Third Party Sensitive data, Restricted Information may be retained on portable equipment only if protective measures, such as encryption, are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment.

All employees and third-party vendors/contractors are expected to adhere to the HR Acuity Bring Your Own Device (BYOD) Policy which includes the following provisions:

- All mobile devices, whether owned by HR Acuity or owned by employees, that have access to company networks, data and systems, are included in the scope of this policy. This includes laptops, smartphones and tablet computers. Limited exceptions to this policy may occur where there is a business need; however, a risk assessment must be conducted by management and written approval must be provided in advance

- The company reserves the right to disconnect mobile devices from company managed networks, infrastructure, applications or services, without notification.

- Lost or stolen mobile devices must be reported to the company immediately. Employees are responsible for notifying their mobile carrier upon loss of a personal mobile device.

- If an employee suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident to the company immediately.

- The employee is expected to use his or her mobile device in an ethical manner at all times and adhere to the company's acceptable use and other applicable policies.

- The employee is personally liable for all costs associated with his or her personal mobile devices.

- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware and/or other software or hardware failures the render the mobile device unusable.

- HR Acuity reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

- No HR Acuity Third Party Sensitive data should be retained on portable equipment.

E. Paper Storage and Disposal

Source reduction of confidential documents -- creating less paper waste in the first place -- is the best way to eliminate exposure of confidential materials and reduce the cost of disposal. HR Acuity promotes this policy.

Recycling is an effective way of destroying documents. Recyclable papers are collected in secured accessible bins, stored in a secure holding container/area and then sent off-site for recycling/destruction. HR Acuity approach is to treat ALL recyclable waste paper as confidential -- a "Universal Precautions" approach to paper -- accomplishing three objectives: minimizes the need for staff to determine if a piece of paper is confidential, fully destroys the document, and minimizes environmental impact by enhancing recycling efforts.

Recycling with a bonded/certified destruction service: Hauling the paper to a bonded recycler or directly to a bonded paper mill for secure shredding.

IX. Incident Response Planning and Notification Procedures

HR Acuity's goal for incident response is to minimize any negative impact to our clients through the use of a comprehensive response and mitigation plan. This plan includes mechanisms for documenting the incidents, determining notification requirements, implementing remediation strategies, and reporting to management.

HR Acuity has a dedicated team and Security Operations Center (SOC) that actively monitors all of our resources to identify potential vulnerabilities and security incidents 24x7x365.

1. In the event of a security incident related to the HR Acuity environment, SOC Team will alert HR Acuity based upon a contact-tree that has been predetermined. This contact-tree is reviewed quarterly to ensure it is up to date.

2. Working with Microsoft we will:

   a) Determine the nature of the attack.

   b) Determine the attack point of origin.

   c) Determine the intent of the attack. Was the attack specifically directed at HR Acuity to acquire specific information, or was it random?

   d) Identify the systems that have been compromised.

   e) Identify the files that have been accessed, determine the sensitivity of those files and which clients have been impacted.

3. The CTO or ISO will immediately notify the appropriate authorities if required and HR Acuity Management Team. Any written communications involving legal counsel should assert attorney-client privilege to ensure strict confidentiality, as appropriate.

4. HR Acuity will then notify the client or clients potentially impacted by the incident. Communications will include the steps being taken with regard to details on incident response, recovery and remediation.

5. If it has been determined that a security breach has occurred, the database and access to the application would be disabled immediately.

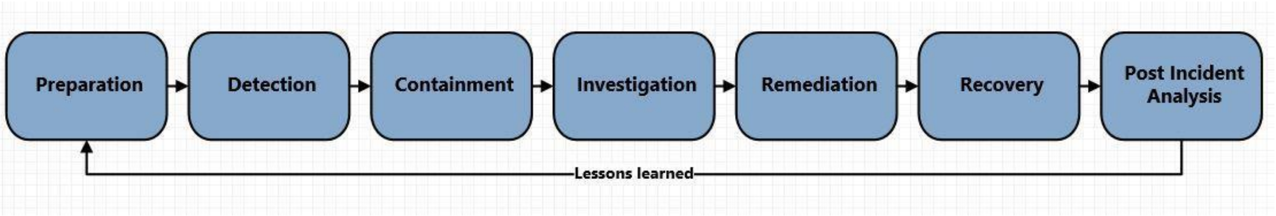
6. HR Acuity would work with its clients to reset all passwords as well as change profiles at the server level.

7. Continued follow up communications with impacted clients will take place with regard to the incident response, investigation into cause of the incident, recovery operations and timeline as well as steps to remediation.

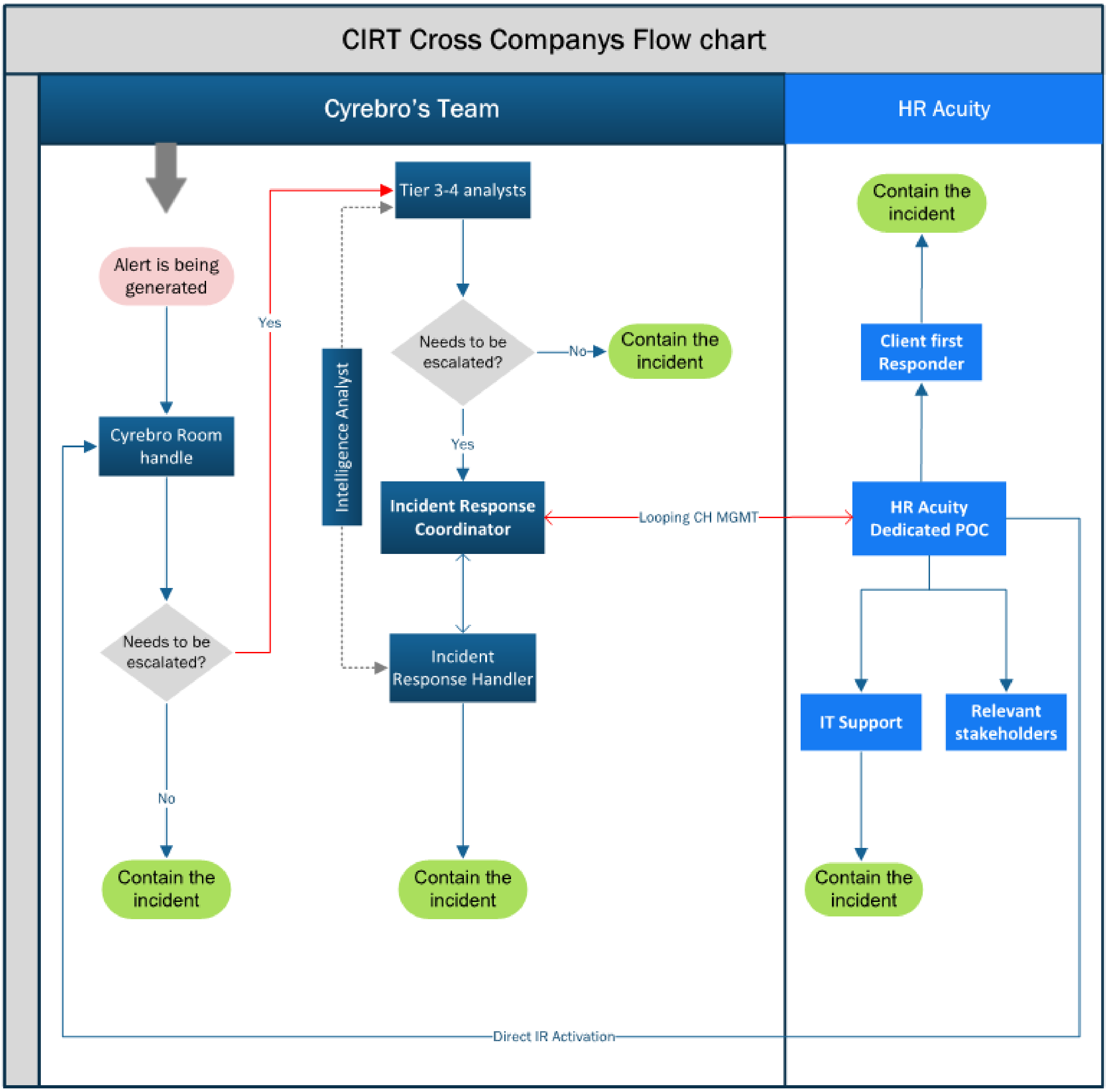
8. In the event of a breach to the security of unencrypted computerized personal information, HR Acuity will work with its clients to notify all impacted individuals whose information is reasonably believed to have been acquired by an unauthorized person.

9. Following the incident, HR Acuity will review the incident cause and response execution. If required, updates or changes to system security to prevent future attempts or breaches. Policies and Incident Plan will be updated as necessary.

Incident Lifecycle and Handling Process



CIRT (Cyber Incident Response Team) Workflow



XII. Education and Training

The ISO and supervisors shall ensure that appropriate security awareness training is routinely conducted for all employees who handle sensitive data using the following educational procedures that have been put in place:

- Training programs will be conducted within 30 days of hire and at least annually for all employees. Program will include a review of HR Acuity security policy, guidelines, procedures, and standards, as well as departmental procedures and best practices established to safeguard sensitive information.

- Training shall be in conformance with regulations governing specific categories of Restricted Information
- Training materials should include topics such as password management and use, best practices for protecting restricted information, incident reporting, and security reminders regarding current threats to technical environments in which individuals are working.

XIII. Third-party Agreements

When providing access to or passing Restricted Information to a third-party agent of HR Acuity, the written contractual agreements should include terms and conditions that:

- Prevent disclosure of Restricted Information by the agent or affiliate to other third parties including subcontractors, except as required or permitted by the approved HR Acuity agreement or contract terms,
- Require all agents and affiliates to observe federal and state laws and HR Acuity policies for privacy and security,
- Require a specific plan by the agent or affiliate for the implementation of administrative, technical, or physical security strategies as outlined in this policy,
- Require a plan for the destruction or return of Restricted Information upon completion of the agent's or affiliate's contractual obligations,
- Specify access or authorization permissions and restrictions necessary to fulfill contractual obligations,
- Require notification of any breach of the security of personal information to the HR Acuity owner of computerized data immediately following discovery if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Access to HR Acuity or derivative information should be terminated when contractual obligations have been completed.

A. Vendor Risk Management

HR Acuity's Vendor Risk Management program is a formal way to evaluate, track and measure third-party risk; to assess its impact on HR Acuity's business; and to develop compensating controls or other forms of mitigation to lessen the negative impact to the business if an incident should occur. A vendor risk management program provides consistency and oversight for managing vendors.

Managing vendor risk is an ongoing process that is based on standardized, repeatable processes that include reviews for continuous improvement. The HR Acuity Vendor Risk Management program is based on the following basic principles.

1. **Perform initial vetting and review of the proposed vendor**

    1. Categorize vendor products and services, determine internal ownership of vendor relationship

    2. Information Security posture review (SOC, ISO, Cloud, On Premise)

    3. If applicable, vendor will be required to complete and submit HR Acuity's Security Questionnaire, which is based on the Vendor Security Alliance standards

        1. If the vendor has a valid third-party audited information security certification (e.g. ISO 27001, SOC 2), then a copy of the certification can be provided and the Documentation and Questionnaire sections do not need to be completed.

        2. All vendors complete the Profile section

        3. Vendors must complete, sign and submit the Documentation and Questionnaire sections **IF**

            1. The vendor does not have third-party audited security certification **AND**

            2. The vendor's services involve transmitting, storing, accessing or processing HR Acuity client data **OR**

            3. The vendor outsources or uses subcontractors in delivery of their services

    4. Contractual review (Deliverables, T&C's, SLA's, Legal & Regulatory, NDA)

2. **Identify potential risks and mitigation controls**

    1. Security and performance (SLA, data sensitivity, incident management)

    2. Access controls (Role based, multi factor authentication, data encryption)

    3. Viability (Review of alternate providers, conformance to required security controls)

3. **Align vendor security control environment with HR Acuity's information security program**

4. **Implement ongoing governance oversight and performance reviews**

    1. Add vendor information to HR Acuity Vendor Tracking database

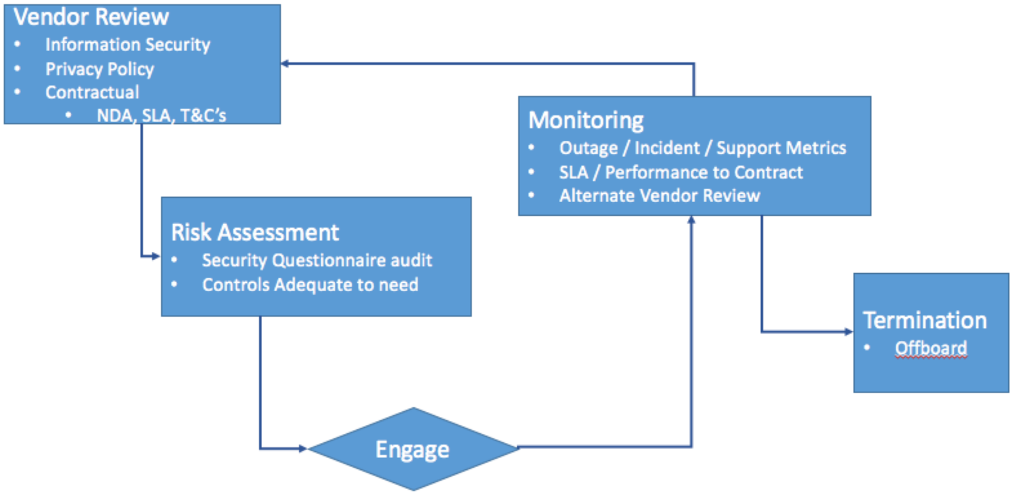
    2. Ongoing analysis and metrics for SLA performance, outages and incidents

    3. Conformance against HR Acuity security requirements

    4. Review of alternative vendors based on performance, features and client needs

5. **Upon contract termination, perform Off boarding tasks related to systems and data access levels**

Vendor Management Process



VI. References

Management Guide for Information Security

ISO 27001

OWASP Guidelines

SANS Security Configuration Guidelines

VII. Revision History

Date of Change	Responsible	Summary of Change
08/01/16	D. Muller	Policy created
09/12/17	D. Muller	Leadership Review/Minor updates
09/17/18	D. Muller	Leadership Review/Updates to: IV.A. Authorized Access: Drug screening V. B. Password Authentication: Credential updates V. C. Session Protection: Length of time
01/07/2019	V. Gupta	Leadership Review/Updates to: III.D. Added Governance section III.C. Risk Assessment IV. Code of Conduct VI.C. System Protection VI.E. Software Development IX. Incident Response planning and notification procedures X.D. BYOD Policy X.E. Paper Storage and Disposal XIII.A. Vendor Risk Program
02/05/2019	D. Muller	Leadership Review; Updated formatting. Minor updates. Removed references to HRAOD (HR Acuity On-Demand)
01/21/2020	V.Gupta	Updated formatting. Minor Updates to Vendor Risk Management. Updated to Patch Management Section
03/31/2021	V.Gupta	Updated Section E with information about Network Vulnerability Tests
03/24/2022	P Witherspoon	Updated for SOC 2 Type 2 Certification

Appendix A. Definitions

Authorized Individual

An HR Acuity employee, contractor, or other individual affiliated with HR Acuity who has been granted authorization by a Data Owner, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with HR Acuity. The authorization granted is for a specific level of access to a Resource as designated by the Data Owner, unless otherwise defined by HR Acuity policy.

Data Custodian

The authorized HR Acuity personnel who have physical or logical control over a specific Electronic Information Resource. This role provides a service to a Data Owner.

Data Owner

The individual designated responsibility for the information and the processes supporting a specific HR Acuity function. Data Owners are responsible for ensuring compliance with federal or state statutory regulations. Responsibilities of Data Owners may include, for example: specifying; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application.

Electronic Information Resource (Resource)

A resource used in support of HR Acuity activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data (in raw, summary, and interpreted form), other electronic files, and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the HR Acuity mission. These resources are valued information assets of HR Acuity.

Encryption

The process of converting data into a cipher or code in order to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher. The keys are binary values that may be interpretable as the codes for text strings, or they may be arbitrary numbers. Appropriate management of these keys allows one to store or transmit encrypted data “in plain sight” with little possibility that it can be read by an unauthorized entity. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party

Essential Resource

A Resource is designated as Essential if its failure to function correctly and on schedule could result in (1) a major failure by HR Acuity to perform a mission-critical function, (2) a significant loss of funds or information, or (3) a significant liability or other legal exposure to HR Acuity or an HR Acuity client.

Restricted Data

Restricted Information describes any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

Restricted Resource

A Resource that supports the storage, transmission, or processing of Restricted Data to which access requires the highest degree of restriction and that requires the highest level of security protection.

Team Member

Employees or third-party contractors/vendors of HR Acuity