HR Acuity Acceptable Use Policy

Document Version	**4.0**
Date	03/01/2022

Document Properties

Property	**Description**
Circulation	Internal Use Only
Classification	Confidential
Document Owner	VP Technology
Last Reviewed Date	03/01/2022
Last Reviewed By	Paul Witherspoon
Next Scheduled Review	03/01/2023

Document Approvals

Approver Name	**Title**	**Date**
Deb Muller	CEO	10/29/18
Vikas Gupta	CTO	01/21/20
Vikas Gupta	CTO	02/01/2021
Paul Witherspoon	VP Technology	03/01/2022

Revision History

Version	**Date**	**Description of Changes**	**Revised By**
0.1	7/27/18	Initial Version, based on previous AU policy dated 10 July 2017	ISMS Manager
0.3	7/27/18	Modified RACI	ISMS Manager
0.4	10/18/18	Added Approval Information	ISMS Manager
1.0	10/29/18	Approval	D Muller
2.0	11/1/18	Change Dropbox to Microsoft Sharefile. Update Section 6. Added Tailgating policy in Section 5	V Gupta
3.0	1/21/20	Added Approval Information	Vikas Gupta
4.0	03/01/2022	Added Approval Information	P. Witherspoon

1 Introduction

1.1 Purpose

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at HR Acuity in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.
HR Acuity provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.
This policy provides management support for proper conduct principles and unambiguously demonstrates to stakeholders the management's commitment to a healthy and productive environment. This policy is both approved and supported by the HR Acuity CEO.

1.2 Background

Acceptable use of company assets requires sensitivity to the HR Acuity environment, responsible stewardship of assets that the stakeholders have entrusted to HR Acuity, and compliance with all legal and ethical responsibilities. The intent of this Acceptable Use Policy is not to impose restrictions that are contrary to HR Acuity's established culture of openness, trust, and integrity, but to ensure the safety and protection of users

and the assets entrusted to them for the benefit of HR Acuity and their customers. Effective security is a team effort that involves the participation and support of every HR Acuity employee and affiliate who accesses HR Acuity information systems. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly.
HR Acuity Information Security must approve exceptions to this policy in advance through written authorization made to the President and CEO, or her designee.

2 Scope

2.1 Users

All employees, contractors, consultants, temporary and other workers at HR Acuity, including all personnel affiliated with third parties must adhere to this policy.

2.2 Systems

This policy applies to information assets owned or leased by HR Acuity, or to devices that connect to an HR Acuity network or reside at an HR Acuity site such as personal mobile devices used to access HR Acuity information systems or networks.

3 Environment

Objective: To establish an environment to optimize the HR Acuity mission.

1. You are responsible for exercising good judgment regarding the appropriate use of HR Acuity resources in accordance with HR Acuity policies, standards, and guidelines. HR Acuity resources may not be used for any unlawful or prohibited purpose.
2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the HR Acuity network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.
3. You are encouraged to report any suspicious or unauthorized use of HR Acuity Confidential, HR Acuity Third Party Confidential, or HR Acuity Third Party Sensitive Data (“Highly Confidential Data”) as defined in the Information Security Terms and Definitions.
4. All entities granted access to HR Acuity information assets shall be required to complete a non-disclosure agreement (NDA) to uphold information confidentiality. Failure to complete the agreement shall result in denial of access.
5. The ability to access information or content, whether internal or external, does not imply any consent regarding the use of such assets.
6. The act of downloading/uploading, creating, and/or displaying items of a pornographic or prurient sexual nature creates an uncomfortable or hostile environment, and such activity is prohibited.
7. The act of downloading /uploading, creating and/or displaying items of a racist or sexist nature, or negatively targeting any identifiable group, can create an uncomfortable or hostile environment, and such activity is prohibited.
8. The act of downloading /uploading, creating, and/or displaying items that elicit an uncomfortable response, or are deemed inappropriate, is prohibited. Management reserves the right to determine what is or is not appropriate.
9. There is no guarantee of privacy while using HR Acuity infrastructure. Information created or stored on HR Acuity equipment is considered the intellectual property of HR Acuity. Management reserves the right to monitor workstation activity and examine incidents on any equipment at any time.

4 Stewardship

Objective: Retain stakeholder trust by demonstrating responsible stewardship toward corporate assets.

1. To the extent technically possible, no Restricted Data will be stored on laptops or other portable devices. However, should any Restricted Data be stored on these devices, the information must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible.
2. All HR Acuity Third Party Confidential and Restricted Data electronically-based exchanges should only be conducted using secure sharing facilities designated and approved by the company. Currently, HR Acuity certifies the use of Microsoft Sharepoint to be used for HR Acuity Confidential Data and HR Acuity Third Party Confidential as defined in the Information Security Terms and Definitions. ShareFile or a pre-authorized equivalent should be used for the exchange of Restricted Data as defined in the Information Security Terms and Definitions.
3. Downloading large or streaming files requires excessive bandwidth. To ensure the availability of HR Acuity information resources for all business needs, all high bandwidth applications shall be justified by business requirements.
4. Attempts to intentionally damage or hinder HR Acuity information resources, such as the introduction of viruses, worms, or other forms of malicious software are prohibited.
5. Uncontrolled software, freely available on the Internet or via other sources, often harbors hidden malicious intent and may result in the inadvertent introduction of viruses, worms, Trojans, and other forms of malicious code. The introduction of ANY software not approved by the Information Security Program is prohibited.
6. Individuals, in the course of their tenure with HR Acuity, may be exposed to protected information and are bound by the requirements of the HR Acuity Information Classification and Handling Standard. Protection requirements specifically address the protection of removable storage media such as USB flash drives, external disk drives, or memory cards.
7. Individuals, in the course of their tenure with HR Acuity, may be issued mobile computing devices such as laptop computers and are therefore bound by the requirements of the HR Acuity Information Classification and Handling Standard and any other Standards applicable to the use of mobile devices. Protection requirements specifically address the concerns of sensitive data resident on portable computing devices at home, in automobiles, or in other areas with marginally controlled physical security.
8. Usage of HR Acuity information resources shall be based upon business requirements. Frivolous usage is prohibited.
9. Information Security is everybody’s responsibility, and it is every individual user’s responsibility to report any real or suspected violation of HR Acuity policies and/or standards.

5 Compliance

Objective: To comply with all legal and ethical responsibilities

1. Unauthorized reproduction of copyrighted works, such as software and documentation, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and installation of any copyrighted software for which HR Acuity or the end-user does not have an active license is an infringement of intellectual property laws and is prohibited. Unauthorized duplication of copyrighted material may subject users and/or the Company to both civil and criminal penalties under the United States Copyright Act.
2. Employees may not duplicate any licenses, software, or related documentation for use either on the Company's premises or elsewhere unless such duplication is expressly authorized by the licensing agreement with the publisher. Employees must not provide licensed software to any outsiders including contractors, customers, or others. Employees are not to reproduce any license of any software on personal computers and devices.
3. You are responsible for ensuring the protection of assigned HR Acuity assets. Laptops left at HR Acuity overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of HR Acuity assets or non-company owned assets used to access HR Acuity information to Information Security.
4. You are prohibited from storing company data on any third-party infrastructure or application not designated or approved by the company.
5. All computers must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the computer is unattended.
6. You must not interfere with corporate device management or security system software installed on computers. Any attempt to circumvent access controls, or "hacking", regardless of intent, is a violation of the federal Computer Fraud and Abuse Act, as well as state and local law, and may subject the violator to prosecution.
7. All non-company owned devices used for HR Acuity work must:
    - Have encrypted hard drives;
    - Have installed a current version of either Norton or MacAfee anti-virus detection software;
    - Family and friends may not be allowed to access your device using the same account established to access HR Acuity information and networks.
8. Desks and work surfaces shall be cleared of sensitive information while unattended and at the end of the work shift prior to leaving.
9. Printers and other devices which could disclose sensitive information in the printed form shall be cleared of such information in a timely manner.
10. Use of HR Acuity communication media, such as email, instant messaging, and group collaboration tools, to send threatening or harassing communications is prohibited and may result in an investigation by relevant law enforcement authorities.
11. Certain employee or customer records, such as Social Security numbers, are protected against unauthorized access. Disclosure, either accidental or intentional, may subject the responsible party to the full measure of recourse.
12. Utilization of HR Acuity information resources for personal gains, such as gambling or self-marketing, is unethical and hence prohibited.
13. Providing information about, or lists of, HR Acuity employees to parties outside HR Acuity is strictly prohibited.
14. Casual and limited personal use of HR Acuity information resources is allowed on a non-interfering basis. Sending and receiving an occasional personal email, and "break time" web surfing may be considered examples of casual personal use.
15. Sharing user accounts and passwords hinders the ability to hold users accountable for their activities and may result in false accusations against the legitimate account holder. Account sharing may also result in identity theft. Sharing of accounts, passwords, and other user access information is strictly prohibited. Therefore, employees must keep passwords secure, and never divulge their passwords to anyone.
16. Tailgating: Do not let unfamiliar persons follow you into private or locked entrances into office space. Our natural inclination is to be polite and hold open the door for the person behind us. ... Be aware of doors that are propped open or unlocked. Notice if security staff are not where they are supposed to be.

6 Electronic Communications

Objective: To limit business risk exposure related to external communications, including social media.

The following are strictly prohibited:

1. The personal use of any chat or streaming media service shall not be permitted without explicit management approval in writing.
2. Sending Spam via email, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
3. Use of an HR Acuity email or IP address to engage in conduct that violates HR Acuity policies or guidelines.
4. Social networking posts must conform to all relevant requirements of both this policy and the Information Security Program.
5. Employees shall not claim to represent HR Acuity in social network postings or messages unless specifically authorized in writing to do so by management.
6. Do not, under any circumstances, defame or otherwise discredit the products or services of the Company, its partners, affiliates, customers, vendors, or competitors.
7. Postings shall not use HR Acuity's logo, trademark, proprietary graphics, or photographs of the Company's premises, personnel, or products without explicit management approval in writing.
8. Postings, whether business-related or personal, must not contain information that HR Acuity considers derogatory or damaging to the company's reputation and goodwill. Any such posts, even those made anonymously, are subject to investigation and appropriate remedial action by the Company.
9. Violations of the above rules may result in both disciplinary actions (recourse), up to and including termination of employment, and remedies in law.

7 Recourse

Objective: To ensure management and adjudication of policy violations

Compliance with this Acceptable User Policy is a condition of resource usage as well as a means for enforcement. Users shall have no expectation of privacy while using HR Acuity information resources and equipment. HR Acuity reserves the right to monitor the usage of HR Acuity information resources and to take relevant disciplinary action. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with HR Acuity.

8 OWNERSHIP AND REVIEW

This Standard is owned by the ISMS Manager.
This Standard shall be reviewed on an annual basis.
Changes to this document shall be in accordance with the ISMS Document and Records Control Standard.

8.1 Contact Information

VP Technology

617-909-7355

pwitherspoon@hracuity.com

8.2 Document RACI

Responsible	Assigned to do the Work	ISMS Manager
Accountable	Final decision, ultimately answerable	ISMS Steering Committee
Consulted	Consulted BEFORE an action of decision is taken (proactive)	Leadership Team
Informed	Informed AFTER a decision or action has been taken (reactive)	Named participants in this document. Other parties affected by the change.