Resonate Inc.

Information Security Policy

Version 2

APPROVALS

Approval Date	April 2022
Policy Owner	VP Engineering
Approving Body	Chief Technology Officer

resonate

Table of Contents

resonate

User Account Management Policy

1. Access to corporate information assets will not be granted or modified for any individual without appropriate authorization from the affected Data Owner(s) and a member of the requester's management staff. IT will maintain the procedures for obtaining owner and management authorization for access to critical information assets.
2. The following procedures will be enforced when creating a new user or system account:
   a) No system or user accounts will be created without proper documented authorization from a manager responsible for authorizing new accounts.
   b) When establishing accounts, standard security principles of "least required access" to perform a function are to be followed, where possible.
   c) Access to any data asset must be approved in advance by the appropriate data owners. Role Based access controls may be used to pre-approve and track access to data assets.
   d) A unique account and password will be issued to each individual authorized to have access to computing and information resources. All accounts must be password protected and no shared accounts will be allowed. (See the Password Management Policy for information on assigning or changing account passwords.)
   e) Remote access can be established when an employee, contractor or business associate of Resonate has a legitimate business need to access Resonate information from a remote location and has the approved equipment and proper authorization. Remote access to web-based email systems is approved for use from non-Resonate equipment. All remote access to Resonate internal systems and networks requires access with approved VPN software.
   f) Vendor accounts used for system support will be enabled only during the time needed.
3. The following procedures will be enforced for changing user or system account privileges:
   a) All password resets require authenticating the user before changes are made.
   b) All changes providing additional access privileges will require prior approval from the user's manager and the appropriate data owners of the assets to be accessed.
4. The following account procedures will be enforced for the termination of workforce members:
   a) When any employee terminates their employment with Resonate, their access to all critical Resonate systems will be revoked as soon as possible.
   b) Revoked or suspended accounts, due to terminations, may only be retained for purposes of transitioning or reassigning the associated application or system data or to comply with documented legal requirements. Any account transition or reassignment must be complete within 90 days of the termination date via a formal account management and approval process. After 90 days, accounts that have not been reassigned will be removed from the system.

5. Other Required Account Management Procedures:
   a) All workforce members who manage or authorize accounts, or who have access to confidential data are required to read and follow this policy. All said workforce members are required to report violations immediately to the IT organization.
   b) A user's identity will be authenticated before providing them account and password details.
   c) All workforce members being granted access to sensitive data must have previously signed a Resonate Confidentiality Agreement, which will be kept on file with Human Resources. Vendors must be covered under a Non Disclosure Agreement executed between their company and Resonate, or themselves and Resonate in the case of an independent contractor.
   d) Account sessions that have been idle for more than 15 minutes must be automatically locked or logged out, requiring the user to re-enter authorization credentials to regain access.
   e) After five (5) unsuccessful account login attempts, the account must be locked out and will require the user to contact IT to unlock the account. This must be enforced automatically by the system where the capability exists.
   f) The IT organization or their delegates will perform annual reviews to ensure this policy is enforced.
   g) Access to any database containing confidential data must be authenticated prior to granting access, including access by applications, database and systems administrators, and workforce members.

resonate

Password Management Policy

Required Password ,:

a) First time passwords must be changed upon first use.

b) All passwords must contain at least eight (8) characters (>12 characters recommended). Where possible, technical controls should automatically enforce password length at the time of creation.

c) All user-chosen passwords must contain at least three of the following four characteristics:

- lowercase letters,
- uppercase letters,
- numbers, and
- special characters (!@#$%^&*()).

Non-alphabetic characters will be distributed throughout the password rather than tacking them on to the beginning or ending of the password, to increase password strength. *(The use of control characters and other non-printable characters is discouraged since password systems do not universally support these characters.)*

d) Passwords must be changed at least every 180 days. Password expiration will automatically be enforced in systems where this feature is available.

e) Resonate employee access uses MFA

f) All Resonate network devices (routers, WAPs, firewalls, network managed devices, etc.,) must have unique passwords or other access control mechanisms. Administrators must change all vendor-supplied default passwords before deploying the vendor equipment into the Resonate network.

g) Users must never share or reveal their passwords except in rare, business critical situations. Resonate will hold the user responsible for all activity performed with their personal user IDs as a result of non-compliance with company policies. Workforce members may not use User IDs assigned to another user unless explicitly authorized by management for a business critical event, and even then, only for a short duration. Once an account password has been shared, it must be changed upon next use and kept confidential by the account owner. Users must not allow others to perform any activity with their user IDs. Similarly, users may not perform any activity with IDs belonging to other users (excepting anonymous user IDs like “guest” and authorized shared-access accounts).

h) Shared or “generic” user accounts and passwords are prohibited, except in the case of a business critical situation, approved in writing by management as noted above. In no event shall sharing of accounts or account passwords be a common or frequent practice.

i) Users must not construct passwords identical or substantially similar to the last four passwords they previously employed. This will be enforced automatically on systems where possible.

j) When leaving their systems, users must lock the screen or log out of the system in such a way as to require users to re-enter their password to gain access to the system. Where technically feasible, systems will be configured to automatically enforce screen locking or account logout after no more than 15 minutes of inactivity by the user, requiring the user to re-enter their authentication credentials to gain access.

Storing Passwords

k) Passwords must be encrypted with approved encryption methods when being stored in a file or transmitted across a network.

l) Users must not store passwords in any electronic file on any computer system (including Mobile phones, USB / "thumb" drives, or other mobile devices) without using approved encryption or hashing methods for the stored passwords. Windows encrypted file system (EFS) or other similar file encrypting systems will satisfy this requirement. Resonate may allow exceptions for approved programs that require storing passwords and other credentials for use in automated interaction with other devices or processes. In those cases, administrators will use compensating controls (including file-system permissions) to protect file confidentiality.

m) To support disaster recovery, Resonate may collect administrative and privileged-access passwords for critical systems in electronic and hard copy format for appropriate safeguarding by Executive Management, the company's Security Officer, or in appropriately controlled escrow. When stored onsite, these passwords should be stored in a locked document safe, with controlled key access.

n) Developers must never hard-code passwords into software developed or modified by Resonate workforce members.

Creating Effective Passwords

a) Workforce members should use difficult to guess but easy to remember passwords.

b) To ensure passwords are difficult to guess, workforce members must not employ words found in the dictionary or common character sequences.

c) Workforce members should not use personal details such as phone number, Social Security number, birthday or spouse or children's name unless interspersed with additional, unrelated characters.

d) Workforce members must not use "Resonate" or any derivation of any name associated with Resonate as part of their password.

e) To facilitate easy-to-remember passwords, workforce members may consider employing pronounceable passwords, using an approach such as the U.S. State Department pronounceable password method, providing they satisfy policy statements listed above.

Additional Password Controls

Forced Password Changes on Termination of Employee with Privileged Access

- Workforce members with privileged or administrative access to Resonate systems and administrative accounts must have their accounts disabled AND passwords changed upon termination.

Suspected Compromise or Disclosure of Passwords

- Whenever an unauthorized party has compromised a system, or system administrators have good reason to believe a system or critical system account has been compromised, system administrators at a minimum, must change all passwords on the affected system immediately and IT must instruct all users to change their passwords on other Resonate systems if those users used the same passwords on both the compromised system and other Resonate systems.

resonate

Secure Communication Policy

- Unauthorized communication of confidential information over the public network, including but not limited to, Trade secrets, customer lists, confidential or sensitive customer information, financial reports not available to the general public, computer source code, and other business sensitive data that may cause damage to Resonate, its business partners, or customers, is strictly prohibited.
- When sending confidential or business sensitive information over public networks, whether in files or in emails, the data must be encrypted using strong cryptography, such as 128 bit SSL, 3DES, 256 bit AES, or similarly approved encryption technologies, to safeguard sensitive customer and Resonate data.
- If sending sensitive data over a wireless network, users must follow the Resonate Secure Wireless Access Policy
- Monitoring of all emails sent through Resonate systems may be performed to protect Resonate's assets. Limited personal use of the Resonate email system is allowed at management's discretion as long as it does not affect work performance, however, workforce members must understand there is no expectation of privacy protection for any use of the Resonate email system. All data sent over the Resonate email system may be kept for an indefinite time, and becomes the property of Resonate.
- Remote access to Resonate's corporate network or production systems must be conducted over secure communications using approved secure communication protocols such as Secure Sockets Layer (SSL), Layer 2 Tunneling Protocol (L2TP), or Internet Protocol Security (IPSec) (e.g. over a VPN).
- All workforce members, and third parties remotely accessing Resonate networks must be authenticated using VPN to ensure the remote user is who they claim to be.

resonate

Data Backup Policy

1. A data backup program will be developed and maintained to address at a minimum, the following:
   - All critical business systems containing volatile data will be backed up on a daily basis by the IT organization responsible for managing the systems. Backups will be performed such that systems can be restored with a loss of no more than 1 business day's worth of data. Differential backups are sufficient for daily backups, provided each critical business system has at least one FULL system backup performed each week.
   - Backup and restore procedures will be designed to support restoring data in the least amount of time possible while still maintaining the security of the data, and conforming to any guidelines that may be defined by business continuity planning.
   - In addition to regular system backups, at least one other safeguard should be employed to allow near real-time restoration of data and to further minimize data loss for revenue generating systems. e.g. Server pool, hardware clustering, and/or real-time media replication such as log shipping, or electronic journaling.

Business units responsible for managing business critical systems must ensure their systems are adequately backed up using procedures that meet the requirements of this policy, to prevent the loss or corruption of data from the following common threats.

2. **Critical Server Backups** - The organization responsible for Technical Operations is responsible for ensuring the daily backups of critical business servers and will retain sufficient logs or reports to verify the systems have been backed up successfully. Daily backups must be either full backups or differential backups.
3. **Identify Backup Failures Daily** - Backup logs or reports will be reviewed daily by the data backup team to identify any backup failures. An exception report detailing the failure to backup any critical files or systems will be provided to management for their review on a daily basis. All critical backup failures must be remedied such that they do not fail to back up the following day. Backup failures of non-critical files or data that do not affect the restoration of the system from tape backup, are not required to be remediated.
4. Email will be backed up by Resonate's 3rd party email provider.
5. All other data backups will be kept for a period of time defined in the Data Retention and Destruction policy, after which the data will be destroyed. Destruction must be sufficient to prevent reading information from the backup media via any known technique.
6. At least once per year, testing will be performed on the backup procedures and backup restoration for critical systems.

resonate

Software Development Lifecycle Policy

To protect Resonate systems from unplanned disruptions or unauthorized changes and potential compromise of critical software business systems, it is the policy of Resonate that:

1. Resonate will document and enforce a standard software development life cycle process, that addresses:
    a. Software change requests - to document what system changes are being requested,
    b. Authorization for software changes – to record what changes have been authorized and by whom they were approved,
    c. Software project planning and management - to track software development activities and document software changes and testing activities,
    d. Standardized, documented, product development processes – to ensure consistency in development processes, reducing errors and omissions that could present a risk to system stability,
    e. Secure programming standards,
    f. Testing and acceptance of software changes before release to production, including testing for common security threats as defined by the OWASP top 10 list,
    g. Maintenance process for software, once released to production.

2. All policies related to the collection or protection of data (e.g., privacy policies), including changes to those policies, that are to be displayed on customer facing web sites, must be reviewed and approved in advance by the CTO.

resonate

Access Control Policy

General Access Controls

1. Resonate grants access to its resources based on a demonstrable business need for access. Access rights will be granted to groups (job roles), and never to individual user accounts.
2. All resources are owned by one or more data owners. Data Owners determine who can access, alter, or delete their resources, and convey this information to the Data Custodians, who are responsible for controlling the access to the data assets in their custody. Data Owners also define the length of time to retain specific data, and when it must be destroyed.
3. Users are granted access rights by:
   - Classifying user jobs into one or more roles, and creating an access group for each role,
   - Requesting access from the data owners to specific resources, for each group, and
   - Assigning users to appropriate groups, where they inherit the access rights of those groups.
4. When setting up group access rights, administrators will adhere to the security principle of least privilege, where groups are granted the least amount of privileges necessary to perform their job functions.
5. When setting up access rights, administrators will establish a “deny all” access policy within the environment, where any right not specifically assigned to a user group is denied.
6. No shared user accounts are allowed. All users must be assigned a unique user account and password such that account access can be traced back to each individual.
7. Annually, Data Owners will review the list of access groups granted access to their data assets, and provide any updates to the Data Custodians to ensure no unnecessary access is provided to their data assets.
8. All generic accounts and passwords will be disabled or modified so that no unauthorized individual can gain access to a data resource via vendor supplied default accounts and passwords.

Remote System Security Controls

9. Resonate workforce members must protect all portable and remote computers under their control used to process company business information with an approved virus protection program and malware protection program, whose virus and malware definitions are maintained at the most current level, and with an approved host firewall program configured to prevent unauthorized use of the machine and unauthorized access to company information.

Supported and Approved Remote Connectivity Options

In efforts to provide employees with the most flexible, secure, and efficient means of remote connectivity, the company provides the following supported and approved remote connectivity options:

10. VPN – Resonate will install an approved VPN client on all company owned systems that have approval to connect remotely. Access to the company's internal network via the VPN client must require a valid username and password.
11. All remote access to the production networks, including for the purpose of administering outsourced systems, will be performed through a VPN connection, or other approved secure communications protocol.
12. Webmail (365 Online) is an option that allows employees to access their email via Microsoft's web version of Outlook. Employees with a valid Windows domain ID/password may access this web client with any supported browser.

Authenticating Remote Users

13. Remote access to company computers and networks requires definitive authentication for all users via VPN.
14. All connections to the company network must use encryption technology such as SSL/TLS or IPSecurity (IPSEC).
15. The Technical Operations team will be responsible for managing encryption technology and devices at Resonate.

resonate

Wireless Networking Policy

1. All WAPs (Wireless Access Points) must be approved in advance by the policy owner, and installed and configured by IT or its delegates, to ensure secure wireless computing. When authorizing use of this technology:
    - A list of all approved wireless access points will be maintained and updated, with both logical address and physical location being documented
    - A list of all users authorized to use the wireless network / device will be maintained
    - All access via the WAP will be authenticated using company approved procedures

Configuring Wireless Networks:

2. Resonate **prohibits** wireless networks secured with WEP.
3. All wireless networks connecting to company networks and systems must at a minimum:
    - Use WPA-2
    - Require pre-shared key (PSK) on guest networks
    - Have all default vendor settings changed (default SSID, passwords, admin account name (if feasible), WPA keys, SNMP community strings)
    - Configure the SSID name to be different from the default SSID name of the device, and not reveal any information about Resonate. E.g. SSID name must not be some derivative or modification of the company name that would enable a hacker to discern that this wireless network attaches or belongs to Resonate
    - Disable all unnecessary services/protocols on the WAP device
    - Where configurable, set the broadcast key rotation time to no more than 60 minutes

4. Enable logging and store wireless network logs on a separate server

Connecting Remotely Via a Wireless Network

5. Resonate requires all remote access via SSL VPN.

Wireless Handheld Devices

6. Wireless handheld devices should be secured if they have access to Resonate networks or store sensitive data. At a minimum:
    - Configure the device such that a password is required to access the device
    - Enable automatic device lockout on the device after a period of inactivity. The period of inactivity should be as short as is feasible, but in no case longer than 1 hour.

resonate

Change Management Policy

- All changes to critical business systems or systems that have a required service level will have changes tracked, authorized, planned, reviewed, tested, and coordinated via a formal, documented change management process and appropriately filled out change request form.

Requesting Changes

- All change requests will be tracked in a change management system (e.g., a ticketing system) whose retention period shall be no less than 1 year.
- At a minimum, the *change request* must specify:
    - the requestor's name,
    - the nature of the requested change and the expected impact of the change,
    - what systems are affected by the requested change,
    - date and/or time when the change is needed,
    - the classification of the change request,
    - authorization field indicating the final approval, rejection, or suspension of the change request, including who authorized the change,
    - the date the change request was approved or rejected,
    - the date the change request was implemented

Classifying Change Requests

Change requests will be classified into three distinct classes, each requiring a specific level of review and authorization. The change request classifications are:

Class	Description	Control Overview
PreApproved LOW risk	The change is a common, standard, low risk operation or maintenance event that is well understood, has low risk, and has a standard procedure defined for making the change. (e.g., Add/Change/Delete accounts, grant more disk space, refill printer paper, etc.) A change event is not required to be scheduled.	• Change request will be tracked in change control system via an appropriately submitted change request form. • Change event must be reviewed & executed by an authorized person normally responsible for this type of activity. • Affected persons will be provided sufficient advance notice of the planned change implementation. and notified of completion of the change event.
Standard Change MEDIUM to HIGH risk	Medium to high risk change, based on scope, complexity, or criticality of the item being changed.	• Change request will be tracked in change control system via an appropriately submitted change request form. • Change event must be planned, reviewed by affected parties, and approved in the regularly scheduled CCB meeting. • Affected persons will be provided sufficient advance notice of the planned change

		implementation. and notified of completion of the change event.
Hotfix Change	Unplanned, urgent changes Customer-affecting or critical system outages	• Written approval may not be required if it meets one or more emergency definitions outlined below. • Emergency change request will be submitted within one business day of work completion. • Scheduled changes that are out of cycle

Pre-Approved Change Requests

- Pre-approved change requests are pre-approved and do not require coordinated scheduling before implementing. This category is reserved for common maintenance and administrative tasks that are low risk, have a small scope, and have a standard documented process defined for the change activity that can be executed as time is available, OR is performed on non-critical, systems such as end user workstations, Development severs or QA / Staging servers.
- A change request form must be filled out by the requestor documenting and requesting the change (e.g., a ticketing system).

Emergency Change Requests

- All Change Requests must be submitted prior to performing any work, with the exception of an emergency situation with a production system that impacts, or is about to impact customers or accepting revenue. For emergency changes, the problem will be fixed as soon as possible and the corresponding emergency change request will be submitted no later than the next business day, documenting why the issue was an emergency, and how the change was authorized. If the emergency occurs after hours, verbal approval from the on-call operations manager must be granted prior to making the change. If the emergency occurs during normal business hours, verbal approval must be granted by the policy owner or their delegate. Resonate defines emergency changes as any of the following:
    - Hardware failure
    - An urgent Security Incident
    - The production site is unavailable
    - Contractual or Legal obligation or Service Level Agreement violation
    - A production issue that is significantly impacting the ability to take revenue
    - A critical resource is at risk of exceeding capacity and would lead to a system outage
- Emergency changes that do not meet the above requirements, require verbal authorization from the policy owner before implementing the change.
- If a change request requires implementation prior to the next review meeting and does not fit one of the categories above, the change request will require written approval from the policy owner to designate it as an emergency change request.

Reviewing Changes

- The Change Control Board (CCB) will be appointed to review all standard, and as appropriate, emergency change requests, and will meet regularly to authorize, review and as necessary plan, the change events.
- Requested changes will be classified as defined above, and standard change requests, and as appropriate, emergency change requests, will be planned (via change proposal documentation), and then submitted to the CCB for review and formal authorization to implement.
- Submitted change request/proposals will be reviewed in the regularly scheduled (CCB) meeting. (If using a separate change proposal form from the change request, it must be linked or tracked by the change request ticket such that its location is readily apparent to an auditor and the form must reference the change request tracking ticket number.) If necessary, the CCB may revise the change proposal to ensure risks, standards, and original intent are more effectively addressed.
- Pre-Approved change requests will be reviewed and / or planned by an appropriate administrator authorized to perform the change event, prior to implementation, to ensure the change request is both appropriate and necessary. This will typically happen outside of the CCB meetings.
- The leader of the CCB may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change negatively impacts a key process such as accounting's quarterly closing, or if adequate resources or skill-sets will not be available (e.g., weekend, holiday, or special event).

Implementing Approved Changes

- Prior to approval, all submitted Change Requests will be tested appropriately to ensure functionality works as designed, before general release to production systems.
- All changes will be implemented by a person authorized and qualified to make changes to the systems being modified.
- Approved changes will be implemented on their scheduled date. If the planned change can not be implemented on the date scheduled, a new implementation date must be scheduled and communicated in advance to all stakeholders. If the planned change will result in taking a production system offline, it must be performed during an outage window that has been pre-approved by the business and the policy owner, unless it is an emergency situation where the system is unavailable or about to become unavailable.
- During and following the implementation of the planned change, the affected systems will be monitored to ensure the change functions as designed.
- Following implementation, the change request form will be updated as appropriate, to reflect the implementation of the change, and all affected stakeholders will be notified of the change request status.

resonate

Vulnerability & Patch Management Policy

IT must be informed of information security issues and vulnerabilities applicable to company computing systems and must know what assets they are responsible for securing. When security issues are identified, IT is responsible for notifying appropriate operations personnel, of the need to patch identified asset vulnerabilities.

Vulnerability Scanning

- Vulnerability tests are performed quarterly.
- All potential vulnerabilities identified through vulnerability scans will be communicated to appropriate personnel within the company for applicability and remediation. All high-risk vulnerabilities must be corrected, subject to the Change Control Policy. Follow up scans will be initiated to confirm compliance with company security standards.

Patching Vulnerabilities

- All security patches, hot-fixes, and/or service packs found to be applicable to company computing resources, must have their source tested and verified, and be applied to systems in scope per the following schedule. As with any change to the environment, the change management process must be followed so that configuration changes are adequately tested before being released into the production environment.
    - Security / Critical patches / updates – immediately or during the next scheduled *outage window,* provided the next outage window occurs within the next 30 days
    - Emergency patches (unplanned, urgent changes) will follow the Change Management Policy where written approval to make the change may not be required if it meets one or more emergency definitions outlined in the Change Management Policy.

- All similar systems (systems with the same operating system major version number) will maintain the same critical patch level unless a documented business case exists.
- The patch history for each system will be maintained for at least one year.
- Patches will be prioritized and tracked, so that critical patches can be applied more quickly, and lower priority patches can be applied later within the defined patch schedule.
- The status of which patches have been applied to which systems along with the date of patch implementation will be tracked so that patch status by system or by specific patch, can be easily ascertained.

resonate

Physical Security Policy

Physical Access

- Appropriate facility entry controls will be used to limit and monitor physical access to systems that store, process, or contain business information.
- Cameras will be used to monitor areas containing business critical servers and this data will be stored for at least three (3) months, unless otherwise restricted by law.
- Physical access to publicly accessible network jacks will be restricted to authorized individuals in the data centers.

Access By Visitors

- Visitor access to company premises will be controlled by requiring visitors to check in with the receptionist and log their visit in a visitor log.
- For outsourced data centers that contain company systems that store, transmit, or process customer data, visitors will be required to check in at an appropriate check in point and log their visit, have a visitor badge issued that must be worn while within the data center, and be escorted by a workforce member or authorized data center escort at all times.
- Before entering areas where company systems process, store, or transmit customer data, visitors must:
  - Have appropriate authorization to enter the facility,
  - Log their visit in a visitor log,
  - Be given a physical token (badge or access device) that expires and identifies the individual as a non-workforce member,
  - Be required to surrender the physical token before leaving the premises, or on the date of expiration.
- All visitor logs will be retained for a minimum of three (3) months and must document at least the following information: date & time of visit, visitor's name, which workforce member is being visited, and the company the visitor represents.

resonate

Anti-Virus & Malware Policy

Computers Requiring Anti-Virus Software

All company servers and workstations, including employees' home computers used to process company information or connect to company networks, must have company approved anti-virus software installed, capable of detecting, removing, and protecting against viruses, spyware, adware, (requirement is for all known types of malicious software to include spyware and adware) and other forms of malicious software.

For Windows data servers it is a requirement to scan system files for viruses but not for individual databases.

For email servers, it is required to scan emails for viruses, malware, phishing, and other known threats.

Anti-Virus Software Requirements

- Anti-virus software installed on company systems must be approved by the policy owner,
- The anti-virus software must function properly (not be turned off),
- The anti-virus software must allow scheduling to run at regular intervals,
- The anti-virus software and virus definition files must support automated updates and must have the latest virus definitions installed,
- The anti-virus software must allow logging events either locally or to a centralized monitoring console.

Virus Monitoring

Workforce members must not disable or otherwise deactivate the virus and malware scanning software on their company provided system. Only authorized IT Operations personnel or their delegates may deactivate the malware or virus scanning software, and then, only for the purpose of performing support operations, after which the scanning software will be reactivated.

A centralized console will collate virus events from company computers and allow monitoring by support staff.

When an infected system is detected, IT Operations staff will immediately isolate malware infected computers from the network until they can verify them as virus-free, and will inform workforce members of the need to not send emails or activate other vehicles typically used to spread viruses, if appropriate.

Email Attachment Virus Prevention

Email attachments consisting of executables and/or known potentially unsafe content will be filtered. Resonate licenses virus and malware protection though Microsoft Office 365.

Responsibilities of Workforce Members

Workforce members are instructed not open files or macros attached to an email from an unknown, suspicious or untrustworthy source. Workforce members should delete these attachments immediately, and empty the “Deleted Items” folder in the email system, and empty the Recycle Bin to ensure the files are removed from their system.

Workforce members must not download files from unknown or suspicious sources.

When workforce member’s suspect their system is infected with a virus or malware program, they will notify the IT organization responsible for handling virus infections.

resonate

Incident Response Policy

- Resonate maintains a formal incident response plan developed and maintained to define specific Incident Response (IR) protocols:
  - Roles and responsibilities
  - Communications protocol and contacts to be notified
  - Procedures to classify and respond to security incidents
  - Procedures to investigate security incidents
  - Procedures to contain security incidents
  - Procedures to recover compromised systems
  - Procedures to preserve evidence
  - Procedures to report on security incidents, and
  - Procedures to learn from the incident to improve future performance of the information security program (e.g., post mortem analysis).
- Incident Response Team Members will:
  - Plan for, resource, and assign appropriate individuals to an Incident Response Team to execute the Incident Response Plan in an expeditious manner
  - Ensure security monitoring systems are in place to detect and report security alerts such that they can be identified and responded to,
  - Designate people to be available to respond on a 24x7 basis to critical incident alerts
  - Ensure post mortem analysis is performed on IR reports, and that appropriate improvements are made to the security program based on the IR recommendations
  - Thoroughly document each reported incident:
    - Details of the reported incident,
    - Chain of events, including date and time of the incident, when and how it was detected, when and how it was reported, and to whom it was reported,
    - Names of systems, applications, or data files affected,
    - IP addresses that were affected,
    - User names and passwords that might have been compromised,
    - Date & times and who was contacted for all communications related to the event
    - Date & times of all activities taken to investigate, contain, or resolve the incident,
    - Who had access to, and who actually accessed resources during the investigation,
    - List of resources backed up or preserved before investigating/modifying resource copies,

    - Amount of total time spent responding to the incident,
- Employees will report suspected security incidents to IT, or its delegates, and cooperate with IR team members as appropriate to facilitate the investigation and contain damage.

resonate

Secure Audit Log Management Policy

Establishing Audit Trails

- A process will be established for linking all access to systems and system components, to an individual user. Particularly so for users who access systems with administrative (root) privileges.
- Automated audit trails will be implemented to reconstruct the following events:
  - All actions taken by any individual with root or administrator privileges
  - All access to audit trails and log information
  - Invalid access attempts, including failed login attempts and failed access attempts to resources
  - Use of identification and authentication mechanisms, including
    - logins, switching to different user account after logging in
    - Changes to user accounts or privileges (creation, modification, deletion)
    - Automatic logout of a user after exceeding a locally defined time of inactivity or excessive login attempts
  - Initialization of audit logs, startup and shutdown of systems or audit functions
  - All access to security files, attributes, or parameters, any actions to circumvent security controls, including access to virus protection software
  - Changes of system time or dates other than by NTP
  - Detection of a virus
  - Communication events of interest, including:
    - Network link failures
    - Device connection failure due to device identification or authentication failure (also known as a failed connection attempt)
    - Network and device connections dropped
    - IP addresses of successful and unsuccessful connections,
    - Changes to network security configuration (e.g., firewalls)
  - Creation and deletion of system-level objects
- For each audit trail event, at least the following information will be logged:
  - User identification
  - Type of event
  - Date & time
  - Success or failure indication
  - Origination of event

- Identity or name of affected systems, component, data, or resources.

Synchronizing Audit Information

- All critical systems for which audit trails are being collected must have their system times and clocks synchronized using the Network Time Protocol (NTP) service.
  - Consideration will be given to synchronize time with the primary ISP, to assist in reconstructing security events that involve or originate through the ISP, such as a Denial of Service attack.

Protecting Audit Information

- All audit trails will be secured from unauthorized alteration, including the following controls:
  - Audit trails must be managed only by authorized staff.
  - Viewing of log files will be limited to those who have a specific job related need,
  - Audit trails will be protected from unauthorized modifications,
  - A copy of the audit information for each system collected, will be promptly backed up to a secured centralized log server, in near real time,
  - Logs for wireless network networks will be copied to a secured server on the wired internal LAN,
  - Logs copied to the centralized log server will include those generated by Firewalls, Intrusion Detection Systems, critical servers, authentication servers, and others as appropriate, to facilitate correlating security events,
  - File integrity monitoring / change detection software will be used on logs so that existing logs can not be changed, other than adding new information, without generating alerts that will be seen by security or operations support personnel.

Reviewing Audit Data

- All audit logs will be reviewed at least daily for anomalies, failed access attempts, and other unusual activity, commensurate with the criticality of the system or data, including:
  - Follow-up on suspicious events such as intrusion attempts, authorized accesses at unusual times, and unusual changes to infrastructure devices. Internal investigations of workforce members should be coordinated with the Resonate General Counsel.
  - Identify, investigate, report, and respond to inappropriate activity.
  - Ensure that audit requirements and activities do not unduly disrupt critical business processes.
  - Identify the individuals performing event analyses. Each shall be independent from those defining audit trail rules. Ensure they are available and that they record who, what, when, where, and why sensitive information is released. Rules-of-evidence integrity must be maintained.

- Document all event capturing and analysis procedures, requirements, and responsibilities, including when to involve data forensic specialists.
- Audit all user activity where risk levels warrant.
- Employ event analysis support tools and/or intelligent methods of correlating log data to detect suspicious activity and reduce the volume of false positives.

- Audit log information will be retained for at least one (1) year, with at least the last three (3) months being retained on line. Other laws and regulations may stipulate other retention periods; always use the most stringent guideline when the data is covered by more than one policy, law, or regulation.

Recommended Audit Reports

The following audit reports should be reviewed daily to identify potential security issues, based on best practices:

1. **Attempts To Gain Access Via Existing Accounts**

   Failed authentication attempts can be an indication of a malicious attempt to gain network access by performing password guessing. It can also be an indication that a local user account is attempting to gain a higher level of permissions on a system. A useful failed authentication report should give an indication of the source IP address of the attempts, and the login names used. A summary report is acceptable.

2. **Failed Resource Access Attempts**

   Failed access attempts are an indication that someone is attempting to gain access to either a non-existent resource, or a resource to which they don't have permissions. Failed access attempts can be an early indication of an attacker probing a system, for example with some form of a vulnerability scanner.

   A failed access attempt report will identify the resource on which the access was attempted, the source IP performing the access attempt, and any applicable account information.

3. **Unauthorized Changes to Users, Groups, And Services**

   Modifying user accounts, group accounts, or system services, may be an indication that a system has become compromised. While legitimate modifications occur in a dynamic environment, these changes warrant more scrutiny as they can be an indication that an intrusion has occurred

   This report should summarize change results by authentication system or host. A summary report identifying the changes, the target system, and the source of the change should be included if possible.

4. **Suspicious Or Unauthorized Network Traffic Patterns**

   Suspicious traffic patterns are those patterns that are unusual or unexpected on the local network. This includes traffic both entering and leaving the local network. This report requires a level of familiarity with what is "normal" for the local network.

Administrators will need to be knowledgeable of local traffic patterns in order to best use this report. Some traffic patterns can be considered to be highly suspect in nearly all environments, such as:

- Inbound ICMP Unreachable Errors
- Outbound ICMP Time Exceeded in Transit Errors
- Unexpected outbound DMZ Traffic
- Outbound TCP/25 traffic from a non SMTP server
- Outbound Internet Relay Chat (6660-6669, 7000, others)
- Unusual bandwidth utilization

Summary reports are most useful, and should include the source & destination IP addresses and ports, host names, and protocols used.

resonate

Network Security Policy

Secure Network Planning

- All active Resonate network equipment will be located in a non-publicly accessible, secured room or facility. Physical access will be governed by the Resonate Physical Security Policy.
- An inventory of all company owned network devices in use will be maintained, including appropriate configuration information for installed hardware and software.
- All changes to network equipment or configurations will follow the Resonate Change Management Policy to ensure separation of duties, authorization, and testing for all changes.
- A demilitarized zone ("DMZ") will be implemented to logically isolate publicly accessible systems from internal company systems, prohibit direct routes for inbound and outbound internet traffic, and prohibit direct public access between external networks and any system component that stores cardholder data.
- A proxy server and /or IP masquerading will be used to isolate internal network connections from the public internet and prevent internal addresses from being translated and revealed on the internet. (Technologies such as network address translation or port address translation, or other technologies that implement RFC 1918 address space should be used.)
- Properly configured network firewalls and routers will be implemented to control and monitor the type and flow of traffic between networks, including annual review of all firewall and router rules.
- All non-console administrative access will be encrypted using technologies such as SSH, VPN, or SSL/TLS (e.g., web based management).
- Network devices will follow the Secure Audit Log Management Policy and log all access through console and aux ports, and all firewall configuration changes to a centralized logging system.
- Network designs must consider network security before physically connecting different networks. In production environments, domains with differing levels of trust will not be physically connected or bridged without passing data through a dedicated interface on a security device such as a firewall.

- ***Minimum Security Baseline Configurations***
- Minimum security baseline ("MSB") configurations will be developed for all routers, firewalls, and other managed network devices. The MSB will be based on one of the publicly recognized security configuration standards, such as those provided by Cisco, NIST, The Center for Internet Security (CIS), or SANS. Once developed, these system configuration "images" will be maintained as new patches and operating system and firmware updates are applied. These configurations must address at least the following:

- All similar systems (similar device, same operating system) will maintain the same baseline configuration including all approved patches and software updates.
- All network equipment supporting account logons will have all default account, password, community strings, and other vendor supplied defaults changed from the default values and all unnecessary accounts removed, before they are installed and connected to the network.
- All network account management will follow the Resonate User Account Management Policy, including but not limited to, requiring unique username and passwords for access and automatically logging out or locking idle sessions after a specified period of time.
- All unnecessary and insecure services will be disabled on network devices before they are installed and connected to the network, including the removal of all unnecessary scripts, drivers, features, subsystems, and file systems. Essentially, the device must be configured to run or support only the specifically allowed services or features, all others being removed or disabled.
- All network devices must have system security features configured to prevent misuse of the device.
- Firewalls will be configured such that they:
    - Mutual Distrust (deny) all networks / hosts, except for:
        - Web protocols: (HTTP / port 80), Secure socket layers (SSL / port 443),
        - System administration protocols: (e.g., Secure shell (SSH), VPNs), or
        - Other documented and approved protocols required for business purposes. i.e., Restrict inbound & outbound internet traffic to ports 80 & 443 and those specifically approved for business use.
    - Restrict inbound internet traffic to IP addresses within the DMZ,
    - Prevent internal IP addresses from entering the DMZ from the Internet,
    - Restrict inbound internet traffic to ports 80 & 443 and those specifically approved for business use,
    - Provide stateful inspection of network packets (aka dynamic packet filtering) so only established connections are allowed into the network,

- All router and managed device configuration files, including start up and normal running configurations, will be synchronized so that similar devices run the same configurations, and configuration files will be stored securely to prevent unauthorized access, alteration or deletion, and will be backed up and stored at an offsite location for disaster recovery support, per the data backup policy.
- Network personnel must securely deploy the NTP service to query only specific NTP servers.
- Network personnel must activate logging with timestamps enabled, so logs are sent to a remote server.

Connectivity with External Networks

Resonate does not connect with any external networks in a peer to peer fashion.

Virtual Private Network Connectivity

Firewalls and routers must expressly permit ACLs that allow VPN traffic.

Network Change Control Best Practices

- Before making any major changes to network configurations or system software, the Resonate employee responsible for such work should perform a backup of the current, running configuration before starting the work. Following this principle will facilitate troubleshooting and quick rollback in the event of problems after the change.

resonate

Secure Server Policy

To facilitate a secure computing environment, Executive management responsible for Information Technology, will ensure that a secure planning and deployment process is developed, maintained, and followed to address security principles during the design, installation, and update of critical business servers, and that minimum security baseline configurations (MSB's) are defined and maintained for each class of server. The process and MSBs must address at least the following:

Secure System Planning

- All Resonate owned business critical servers will be located in a non-publicly accessible, secured room or facility. Physical access will be governed by the Resonate Physical Security Policy.
- An inventory of all Resonate owned servers will be maintained, including appropriate configuration information for installed hardware and software.
- All critical servers will be backed up following the Resonate Data Backup Policy.
- All changes to business critical server configurations will follow the Resonate Change Management Policy to ensure separation of duties, authorization, and testing of all changes before release to production environments.
- A proxy server and /or IP masquerading will be used to isolate internal systems from the public internet and prevent internal addresses from being translated and revealed on the internet.
- Descriptions of groups, roles, and responsibilities for logical management of business critical servers will be developed and maintained.
- All non-console administrative access will be encrypted using technologies such as SSH, VPN, or SSL/TLS (e.g., web based management). Remote administrative access will be controlled to a specific list of hosts requiring approval from the policy owner, or their designated Information Security leader. This list of remote administrative machines may only contain hosts or networks internal to Resonate.

Minimum Security Baseline Configurations

Minimum security baseline configurations will be developed for all business critical servers. The MSB will be based on one of the publicly recognized security configuration standards, such as those provided by Microsoft, NIST, The Center for Internet Security (CIS), or SANS. Once developed, these system "images" will be maintained as new patches and operating system updates are applied. These configurations must address at least the following:

- All like systems (similar device, same operating system) will maintain the same baseline configuration including all patches and software updates.
- All servers in scope will have all default account, password, and other vendor supplied defaults changed from the default values and all unnecessary accounts removed, before they are installed on the network.

- All servers in scope's account management process will follow the Resonate User Account Management Policy.
- All unnecessary and insecure services and protocols, and those services not specifically allowed, must be disabled before the servers are installed on the network, including the removal of all unnecessary scripts, files, tools, drivers, features, subsystems, and file systems. Essentially, the server must be configured to run or support only the specifically allowed services or features, all others being removed or disabled.
- All servers in scope must have system security features configured to prevent misuse of the device.
- All servers in scope's configuration files (images) must be synchronized so that similar servers run the same configuration image. Images will be stored securely to prevent unauthorized access, alteration or deletion.
- Network time Protocol (NTP) will be used synchronize servers in scope's times & clocks.

- ***Connectivity with External Networks***
- Resonate does not connect externally with any networks in a peer to peer fashion.

- ***Server Status Monitoring***
- Servers must be configured so they are visible to Resonate network management systems. Common status metrics, such as CPU utilization, page faults, disk utilization, and network usage must be monitored at regular intervals not to exceed 15 minutes in between checks. Resonate will retain historic information for at least 12 months to aid in performance baselines and capacity planning efforts.
- If an insecure protocol such as SNMPv1 or v2 is used, implementation must use the following practices:
- SNMP access will be denied from the Internet and other less trusted networks.
- Monitoring access will be limited to specific internal hosts.
- Disable read-write access and explicitly allow read-only.
- Physical location, contact info and other pertinent information will be included as necessary.

Server Upgrades and Patches

- Servers must follow the Resonate Patch Management policy to ensure the latest approved vendor security patches are tested and installed in a timely manner.

Virus Protection

- All Windows servers must have virus protection configured and enabled and must have the system configured with the latest virus and malware definitions. The system must be configured to log the identification of any viruses the software finds.

resonate

Secure Desktop & Laptop Policy

To facilitate a secure computing environment, Executive management responsible for Information Technology, will ensure that a secure planning and deployment process is developed, maintained, and followed to address security principles during the design, installation, and update of desktop and laptop systems in scope, and that minimum security baseline configurations (MSBs) are defined and maintained for each class of desktop and laptop computer. This process and MSBs will address at least the following:

Secure Desktop & Laptop Computer Planning

- Description of groups, roles, and responsibilities for logical management of desktop & laptop computers will be developed and maintained.
- An inventory of all Resonate owned desktop & laptop computers will be maintained.

Minimum Security Baseline Configurations

- Minimum security baseline configurations will be developed for all desktop & laptop computers. The MSB will be based on one of the publicly recognized security configuration standards, such as those provided by Microsoft, NIST, The Center for Internet Security (CIS), or SANS. Once developed, these system "images" will be maintained to include new patches and operating system updates that are applied to deployed systems. These configurations must address at least the following:
- All like systems (similar device, same operating system) will maintain the same baseline configuration including all patches and software updates.
- All unnecessary and insecure services and protocols, and those services not specifically allowed, must be disabled before the desktop & laptop computers are installed on the network, including the removal of all unnecessary scripts, drivers, features, subsystems, and file systems. Essentially, the desktop & laptop computers must be configured to run or support only the specifically allowed services or features, all others being removed or disabled.
- All business desktop & laptop computers must have system security features configured to prevent misuse of the device.
- A host base (personal) firewall program will be installed, securely configured, and enabled at all times on any Resonate owned desktop or laptop computer that directly connects to the internet, via wired or wireless networking, as well as on any workforce member owned systems that access Resonate networks or systems.

Storing Sensitive Data on Resonate Workstations

- Access to sensitive data will be limited to only those whose job requires access.
- Critical and sensitive business data stored on desktop and laptop computers will be appropriately protected from unauthorized access, and will be backed up regularly to prevent data loss.

Desktop & Laptop Computer Upgrades and Patches

- Desktop & laptop computers must follow the Resonate Patch Management policy to ensure the latest approved vendor security patches are installed no later than one month following their release.

Virus Protection

- All desktop & laptop computers must have virus protection configured and enabled and must have the system configured with the latest virus and malware definitions. The system must be configured to log the identification of any viruses the software finds.

Additional Security Precautions for Laptops

- All laptop computers must be configured for additional security when taken off company premises. Specifically, any sensitive data must be encrypted to prevent theft or unauthorized access. Microsoft Encrypting File System (EFS) is acceptable, assuming a strong user account password has been chosen. A strong password is as defined in the Resonate password policy.
- When booting up or returning from hibernation or sleep mode, laptops must be configured to require manually re-entering the users' password.
- Physical security of laptop computers when taken off premises will require additional scrutiny as these systems are easily stolen. Users must take reasonable precautions to minimize the risk of physical theft when the computer is taken off Resonate premises.

resonate

Security Monitoring & Testing Policy

The company will ensure that an information security monitoring and testing program is developed, maintained, and resourced. The monitoring and testing programs must at a minimum, address the following:

- Test security controls, limitations, network connections, and restrictions annually.
- Internal and external network vulnerability scans will be run at least annually, and after any significant change in the computing infrastructure.
- External facing web application scans will be run at least annually.
- External vulnerability scans when run, must be conducted by a third party company that specializes in this type of service.
- Penetration testing of the computing infrastructure (external facing network scan and application scan) will be conducted annually and after any significant change in the computing infrastructure.

resonate

Information Security Awareness Policy

Information Security Awareness Training

Workforce members must be informed of information security risks and vulnerabilities applicable to Resonate computing systems as well as the need for the protection of customer data and confidential company data. An educated workforce is one of the most cost effective investments in data security, creating a strong deterrent to “social engineering” and other security attacks, while enhancing the effectiveness of all other security controls.

Resonate will implement an information security awareness program for all workforce members, to ensure they are:

- Aware of information security risks, threats, vulnerabilities, and risky behaviors that can lead to a security breach,
- Aware of applicable laws and regulations related to the protection of customer data, and sensitive data,

- Regular updates on security and data privacy issues will be provided to workforce members as needed, to ensure they maintain a high level of security awareness and are aware of new or developing security threats. Particular emphasis should be placed on the protection of confidential and business sensitive information, and how to report security vulnerabilities they identify.

Employee Screening

- Potential workforce members will be screened (criminal background check) to minimize the risk of security breaches from internal resources.

Training

- Annually, training on new information security risks, techniques, and capabilities will be required of, and provided to, those personnel directly responsible for the day to day information security activities within Resonate.

Asset Management Policy

Asset Management System

Resonate will implement and maintain an asset management program that addresses the following:

- Secure asset acquisition process – to ensure security is accounted for when purchasing assets, and that assets are securely introduced into the computing framework, and that asset tracking information is updated in a reasonable time frame and is configured per the appropriate Minimum Baseline Configuration Standard.
- Secure asset tracking and tagging process – to ensure all authorized assets in the computing framework are accounted for, and at a minimum, have the following asset information tracked:
    - Asset description,
    - Asset class, manufacturer, model number, serial number,
    - Physical location of the asset,
    - The latest version number of the operating system and/or firmware installed, including all patches, and service packs, and
    - The designated business and technical owners empowered to make business and technical support decisions for the asset.
- Secure asset disposition process – to ensure assets are disposed of in a secure manner and asset tracking information is updated in a reasonable time frame and follows the Record Retention Policy.

resonate

Connected Entity Policy

- Business managers who arrange or approve third party entity connectivity will arrange for a formal risk assessment of the entity by IT Infrastructure prior to agreeing to provide the connectivity, to ensure proper due diligence has been performed regarding the security risks to cardholder data associated with providing the connectivity.
- Before providing connectivity, the entity must demonstrate it is PCI DSS compliant or provide assurances and contractually assume all responsibility for protecting cardholder data to the same degree as defined by the PCI DSS.
- Workforce members responsible for providing network connectivity to connected entities will maintain a list of all entities who are provided connectivity to Resonate networks or systems, including to which systems the entity has access.
- Personnel responsible for connecting and disconnecting the entity must follow a documented and established process when connecting and disconnecting the entity.

resonate

Change Log

Date	Changes	Author(s)	Comments
April 2017	Initial Document Published	VP Engineering/CTO	
April 2018	Review Policies	VP Engineering/CTO	
April 2019	Review Policies	VP Engineering/CTO	
April 2020	Review Policies	VP Engineering/CTO	
April 2021	Review Policies	VP Engineering/CTO	Vendor Management Policy (External)
April 2022	Review Policies	VP Engineering/CTO	