RESOLUTE®
BUILDING INTELLIGENCE

System Security Practices

WHITEPAPER

TABLE OF CONTENTS

1.0 COMPANY OVERVIEW

Resolute Building Intelligence (Resolute®) provides cloud-based analytics and Resolute Building Intelligence, LLC ("Resolute" or "Company") provides a comprehensive building optimization solution that helps customers transform their buildings from costly necessities into productive business-driving assets. At the core of the solution is Resolute Cloud, a cloud-based software platform that improves building performance through deep operational visibility, powerful analytics, and predictive analysis. The solution helps to reduce energy costs, improve operations, enhance equipment performance and extend equipment life, better manage service needs and SLAs, prioritize capital expenditures, and enable informed business decisions.

Resolute Cloud collects disparate building automation system (BAS) and device building performance data at the building level or across entire portfolios. The BAS and device data is aggregated and run through the Resolute Cloud analytics software. Resolute Cloud transforms the data into insights and actionable strategies to drive improved building performance and decision making.

2.0 SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Resolute provides building management software applications, called "Resolute Synergy" and "Resolute Fusion" or generically: "Resolute Cloud", to its users. Resolute uses on-premise devices to collect environmental data at user facilities. This data is loaded into the Resolute Cloud application for analysis by external users

- **Data Security** - Resolute commits to securing the Resolute Cloud application.
- **Application Uptime** - Resolute commits to providing 99.95% uptime for its
- Resolute Cloud application.
- **Notification of Changes** - Resolute commits to notifying impacted users in the event of a change in commitments through statements of work and master service agreements.

Resolute has established operational requirements that support the achievement of security commitments, as well as relevant laws and regulations. These operational requirements are communicated through Resolute's policies and procedures and as mindful stewards of customers' information. Principal system requirements include:

- **Secured Connections** - Resolute has implemented VPN tunnels to secure the connections from the Resolute Cloud to user facilities.
- **Preventing Inbound Access** - Inbound port access has also been disabled to prevent Resolute devices from connecting to user networks.

- **Restricting User Access** - Resolute performs annual user access reviews to ensure access to the Resolute Cloud environment is restricted to authorized users only. Firewalls are in place for devices located at user facilities to prevent unauthorized access.
- **Monitoring of Hosted Environment** - Resolute monitors reports from AWS monthly to track system performance. Resolute also uses separate monitoring applications to monitor availability. Resolute reviews AWS' SOC report annually to ensure environmental and physical security controls are in place.

2.1 Subservice Organizations

In conjunction with established Resolute controls, certain controls at subservice organizations are necessary to provide reasonable assurance that Resolute service commitments and system requirements will be achieved. These complementary subservice organization controls and the related trust services criteria are described below. Subservice organizations are responsible for implementing such controls. Resolute uses Amazon Web Services (AWS) (subservice organization) for data center hosting services.

APPLICABLE TRUST SERVICE CRITERIA	EXPECTED CONTROLS TO BE IMPLEMENTED BY THE SUBSERVICE ORGANIZATION
CC 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	• Logical access is restricted to necessary personnel only. • Periodic user access reviews of users with logical access are performed.
CC 6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	• All entrances to the building and data center are locked and access is properly restricted. • A user access review of individuals with access to the data center is performed and reviewed.
CC 6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	• Server hard drives are destroyed in a secure manner when no longer in use.
CC 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	• Antivirus software is installed on servers used to provide cloud hosting.

AVA 1.2: The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The following controls are in place within the data center: • Equipment kept on racks • Smoke and fire detection system • Fire suppression system • Fire extinguishers • Dedicated A/C • UPS – tested at least quarterly • Generator – tested at least quarterly • Environmental monitoring software exists, and alerting is in place • Business continuity and disaster recovery plans are updates at least annually

2.2 Data Privacy

Resolute respects privacy and is committed to protecting it through compliance with our Privacy Policy, available at www.resolutebi.com/privacy.

3.0 MANAGEMENT PROCESSES

3.1 Control Environment

3.1.1 Commitment to Integrity and Ethical Values

An ethics policy and a mission statement have been defined by Executive Management as a part of the Employee Handbook. All new hires are required to acknowledge the handbook within one day of hire. The Technology Security Policy and Employee Handbook address workforce conduct standards and sanctions that could be enforced if security and availability standards are violated. The Technology Security Policy assigns responsibility for system security and availability including the performance of internal controls to the CTO and CISO.

Roles and responsibilities are defined by Executive Management in written job descriptions for all employees.

3.1.2 Oversight Responsibility and Structure

The Board of Directors is responsible for oversight of internal controls. The CTO and CISO are not part of the Board of Directors. Results of internal control monitoring assessments are reported to the Board of Directors annually by the CFO or the CEO. Reporting lines are defined by senior management and documented within the organizational chart.

3.1.3 Commitment to Competence and Accountability

Prospective employee qualifications are evaluated during the hiring process by the hiring manager. New hire technical evaluations and reference checks are performed by a third party prior to hire, as applicable. Technical evaluations are performed by Resolute based on source of employee referral and job position. A performance appraisal is completed for each employee annually. Performance appraisals include an evaluation against internal control responsibilities.

3.2 Risk Assessment

The Risk Assessment Procedure defines the objectives, scope, and frequency of the risk assessment. The Director of DevOps and the Consultant review the risk assessment annually. The risk assessment evaluates the following items:

- Potential threats and associated risks
- Probability of threats
- Significance of threats
- Identification of responses to risks
- Tolerance level for acceptance of risk
- Mitigation
- Residual Risk
- Risks Related to Fraud
- Information technology general controls and preventative, detective, automatic and manual controls that contribute to the achievement of objectives.

The annual risk assessment review examines comprehensive areas of risk for compliance with respect to the performance of controls, including the use of unreliable information.

3.3 Information and Communication

3.3.1 Internal User Communication

Company policies and procedures (including security and availability policies) are communicated via the intranet. The Technology Security Policy is signed by all new hires upon hire. Additionally, PhishingBox application is utilized as a security training platform. Security Awareness Training is performed by the Head of DevOps for all new employees and participation is tracked in the application.

3.4 Monitoring

AWS Trusted Advisor, a monitoring service from Amazon Web Services that monitors system performance and security, is aggregated into a monthly summary report and reviewed by the Director of DevOps.

Guard Duty, DataDog, and Trusted Advisor management software internal monitoring applications are in place to monitor system security and availability. The outputs of these applications are reviewed by the security team monthly. Audit logging is in place via Guard Duty. Failure alerts are sent to the DevOps team and resolved, as necessary. Resolute has defined alerting rules through the DataDog application. Alerts are sent to the DevOps team in the event a rule is not functioning. The DevOps team is responsible for investigating alerts received for rules not functioning.

4.0 CONTROL ACTIVITIES

The security committee meets monthly to review internal controls, discuss any changes to the business objectives and their impact on security and availability. This meeting is attended by the Director of DevOps, the Consultant, and other executive management when available. An acquisition and procurement methodology (Resolute Building Intelligence Hardware, Software, and Technology Services Acquisition Methodology) for information systems has been developed by the Chief Administration Officer. The Technology Security Policy includes; responsibility for security of the system, acceptable use policy, sanction policy, and incident response procedures.

4.1 Access and Logical Security

Administrative access to the Resolute Cloud is restricted to authorized employees through the administrative authority group. Access to the production and development root accounts require dual factor authentication. A user ID and password are required to log into the Resolute Cloud. The Information Security Policy documents the use of shared accounts is prohibited. The following default authentication parameters are currently in place for Resolute Cloud users:

- Complexity enabled
- Minimum of eight characters
- Account Lockout: 20 attempts

When a new employee is hired, approval from the Director of DevOps is required to gain access to the Resolute Cloud. The approval is documented in the JIRA ticketing system. Terminated users' access is removed within one business day and documented within an offboarding ticket. An annual user access audit of all in-scope systems is performed by the CEO. External system users (clients) are given a superuser account to their Resolute Cloud area upon onboarding. The superuser account administration is granted during the final stages of implementation and is approved by the client.

4.2 Procedures

The network and application diagrams document the network devices and firewalls.

Multiple firewall devices are configured to restrict access to the Resolute Cloud and RGA devices. Firewall rule sets are reviewed by the DevOps team annually as part of the Annual Security Review Meeting. The RGA device firewalls are configured to be fully closed as the default setting. Administrative access to the firewall is limited to members of DevOps. Firewall logs are retained. These logs are monitored by the DevOps team when issues are identified in system performance or security. Alerts are in place for changes to the firewall rules. Alerts are sent to the DevOps team. The DevOps team is responsible for investigating and resolving alerts. Customer deployments follow a standard configuration for software and equipment. Only the firewall for each customer is customizable.

Connections to hosts are encrypted via certificates and TLS. End-user and server workload traffic is segmented by IP address to support customer data isolation.

In legacy customer environments Resolute Cloud obtains its information from JACE devices located throughout the customer facilities. The JACE devices receive information from the building and report to the RGA.

JACE devices do not have inbound port access from the internet. The RGA sends this data to Resolute Cloud for use within the software. For other customer environments, the customer provides the data directly to Resolute Cloud.

Remote access for RGA devices is disabled except via VPN. The passwords for these devices are stored in LastPass. Access to the passwords is restricted to the Client Services Manager and authorized members of the DevOps Team. A VPN tunnel is established from inside the customer network to report outbound to the cloud. There is no inbound traffic to the customer network. For client using Haystack, Resolute will set up a VPN tunnel with an administrator account to connect haystack servers with Resolute Haystack servers.

Public and private encryption keys are used to control all access to production and development resources. AWS key management system is used to rotate encryption keys. Backups of customer metadata are encrypted. Encryption keys are not stored in clear text.

4.3 Data Security

Hard drive encryption is installed on all development laptops during the computer setup process. Decommissioned workstations are stored by Office Management and disposed of, as needed. Decommissioned workstations to be destroyed, are documented and scrub of all data prior to destruction.

4.4 Antivirus

Antivirus definition files are updated hourly. Antivirus reports are reviewed monthly to ensure antivirus is installed on all devices and that definition files are up to date.

This review is performed as a part of the monthly security meeting. This meeting is attended by the Director of DevOps, the Consultant, and other executive management when available.

4.5 System Operations

The Incident Response Plan documents the process of responding to security events, security incidents and business disruptions, roles and responsibilities, recovery procedures, and reporting. Security events are tracked to resolution by IT and documented in the ticketing system. Security incidents are tracked to resolution by IT and documented in the ticketing system. A root cause analysis is performed for all security incidents.

4.6 Change Management

A change control process is defined within the Development Change Control Workflow document. Changes are requested by product owners and assigned to developers by the Development Lead. The developers and product owners together create change requirements. Development is tracked to implementation in JIRA. Changes deployed to production environments are:

- Authorized during the monthly sprint planning meetings.
- Bug fixes are tested by the product team to confirm the changes will behave as expected when applied and will not adversely impact performance.
- New features are also tested by QA personnel for each release.
- Approved during the Go/No Go meeting to provide appropriate oversight and understanding of business impact.

The final approval is obtained during the meetings. Emergency changes, referred to as hotfix changes, are changes implemented between biweekly releases. Any hotfix changes must be approved by the Director of Development prior to implementation. Application of security patches to all servers and workstations are implemented monthly. Patch installation is monitored monthly by the DevOps team. Segregation exists between development and production environments.

Baseline configurations are maintained within AWS for servers. RGA and JACE configurations are also maintained. Changes to the Baseline, RGA and JACE configurations must be approved by the CISO.

4.7 Risk Management

Resolute has a cyber insurance policy in place. A review of the AWS SOC report is performed annually by the Security Consultant to ensure controls are operating effectively.

A vendor risk assessment is performed by the Director of DevOps and Consultant annually and includes the following:

- Vendor type
- Business impact risk
- Risk scoring
- Risk mitigation (high-risk vendors)

4.8 Availability

Resolute utilizes a web load balancer to monitor and promote availability and reliability of the system. Database backups are performed daily. RGA configuration files are static and are backed up remotely for offsite storage. Failed backups create alerts, which are monitored by the DevOps team. Business continuity and disaster recovery plans are established and reviewed annually. Backup restorations are performed at least annually by a member of the DevOps team.

5.0 SYSTEM COMPONENTS

5.1 Infrastructure

The Resolute Cloud environment is entirely hosted by Amazon Web Services. Data is uploaded to the Resolute Cloud environment through two different methods. For legacy clients that utilize the RGA devices, these devices are located at the client's facility and interface with Java Application Control Engine (JACE) devices that are connected to environmental systems at the client facility. The physical security of these devices is the client's responsibility. For other clients, a virtual machine is setup by the client using Haystack and connects to the Resolute Cloud environment in the place of the RGA device.

5.2 Software

The primary application in scope is the Resolute Cloud™ System (Resolute solution). Resolute uses the following software to support the Resolute solution.

- **DataDog** – Cloud monitoring
- **Ansible** – IT Automation for configuration management
- **LastPass** – Password management
- **Bit Defender** – Anti-virus and malware protection
- **JIRA** – Ticketing software
- **AWS Key Management** – Encryption key management
- **PhishingBox** – Security awareness training
- **GuardDuty** – Threat detection

5.3 People

The Resolute personnel supporting the Resolute solution are divided into the following groups:

- **Engineering** – Responsible for the integration of the system
- **Product** – Responsible for the maintenance of the system
- **Development** – Responsible for the development of the system
- **Client Support** – Responsible for the successful use of the solution
- **Human Resources** – Responsible for employee onboarding and annual performance evaluations
- **Board of Directors** – Ultimate responsibility for the security and availability of the system

6.0 COMPLEMENTARY USER CONTROLS

Management of Resolute assumed, in the design of Resolute's Resolute Cloud System that certain controls will be implemented by user entities, and those controls are necessary, in combination with controls at Resolute, to provide reasonable assurance that Resolute's service commitments and system requirements would be achieved. These complementary user entity controls and the related trust services criteria are described below.

User entities are responsible for implementing such controls. User entities are responsible for approving creation of the superuser account. Common Criteria 6.2

7.0 USER ENTITY RESPONSIBILITIES

User entities may have responsibilities when using the system. Those responsibilities are necessary for the user entity to derive the intended benefits of using the services of Resolute. User entity responsibilities are as follows:

- User entities are responsible for restricting client-initiated network changes to the RGA and JACE devices once implemented within their network.
- User entities are responsible for distributing and maintaining user access for their organization.
- User entities are responsible for the physical security of the RGA and JACE devices once implemented within their facility.

RESOLUTE®
BUILDING INTELLIGENCE

Optimizing HVAC System Performance

Analytics-powered software backed by extensive engineering expertise

SOC-2 Compliant

The Gold Standard
of Data Security

PRIVACY
SECURITY
AVAILABILITY
PROCESSING INTEGRITY
CONFIDENTIALITY
AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

Solving real-world problems
with real-time answers

Resolute Building Intelligence LLC

1849 W. Maple Road
Suite 130
Troy, MI 48084

(888) 798-6699
hello@resolutebi.com
www.resolutebi.com

BIG DATA, SOFTWARE, & BUILDING EXPERTS

Resolute was founded by tech-industry veterans with extensive experience developing big-data, cloud-based software solutions for large enterprise customers across multiple verticals such as real estate, banking, transportation, manufacturing, and others. Many of our team members are former employees of Compuware Corporation, a $2B+ enterprise software company that pioneered the use and analysis of data to build, test, and manage business-critical applications for 90+ percent of the Global 100.

The Resolute technology team includes highly skilled software developers, energy engineers, system integrators, and analytics experts. This unique blend of talent comprises the core competencies, skills, and experience needed to build an innovative and intuitive analytics solution powerful enough to competently address today's complex building-performance challenges.