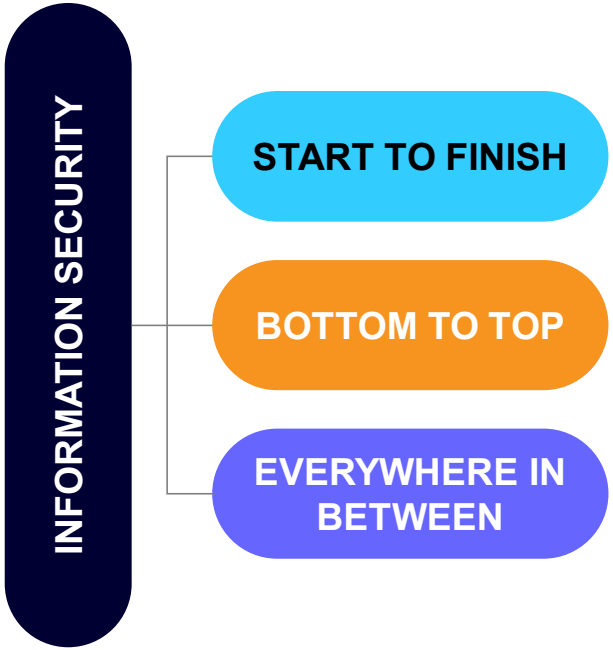
Acumatica
The Cloud ERP

Acumatica Information Security

Information security is a risk management imperative that “software as a service” providers, like Acumatica, share with customers.

We all have an interest in protecting private personal data along with confidential business information. That is why we have dedicated substantial resources to establishing and maintaining a comprehensive information security program. Our program is designed not only for basic compliance with legal and regulatory requirements, like the European Union’s General Data Protection Regulation (“GDPR”), but for consistency with internationally accepted standards of best practices like SSAE and ISO IEC 27001:2013, as well as other authoritative sources of information security and data privacy best practices guidance.



Acumatica takes a *layered, defense-in-depth approach* to protecting the confidentiality, integrity and availability of systems and data, by deploying administrative, technical and physical controls.

For obvious reasons, we don't disclose sensitive details about our information technology security environment that could help a malicious attacker succeed. This document is intended to provide a picture of the contours of our information security program, along with a few highlights of the secure foundation upon which our software and services are built and delivered.

From design through development and on to implementation, our ERP solutions are created through secure processes in secure environments.

By hosting our SaaS in Amazon Web Services ("AWS"), we provide our customers with the significant security benefits that come with *the most advanced cloud computing infrastructure on the planet*. Aside from the formidable infrastructure and platform security elements inherent to AWS, Acumatica has architected its services to segregate and isolate different Acumatica customer environments. Administrative access to Acumatica's AWS management console is strictly limited to a handful of Acumatica key personnel on the basis of "need to know" and "least privilege" principles and even so requires the use of *Multi-Factor Authentication* to gain entry.

Acumatica employees with these privileges, as well as those who support customers and may need to access customer databases for support purposes, can only do so through encrypted channels via an Acumatica IP address.

This means that Acumatica's access to a customer database for support purposes requires a connection through either an Acumatica physical facility or office or the Acumatica VPN, which uses secure protocols TLS 1.2 or IPSEC. The data associated with any activity in these channels is logged and monitored by our information security team. Customers control access rights and management within their dedicated Acumatica SaaS environment by assigning access credentials and can further delineate access by IP address.

Information Security Management

FRAMEWORK

Acumatica's information security management framework consists of security policies, standards and procedures.

Specific information security roles and responsibilities are assigned for the management of the information security program.

These information assets include, but are not limited to:

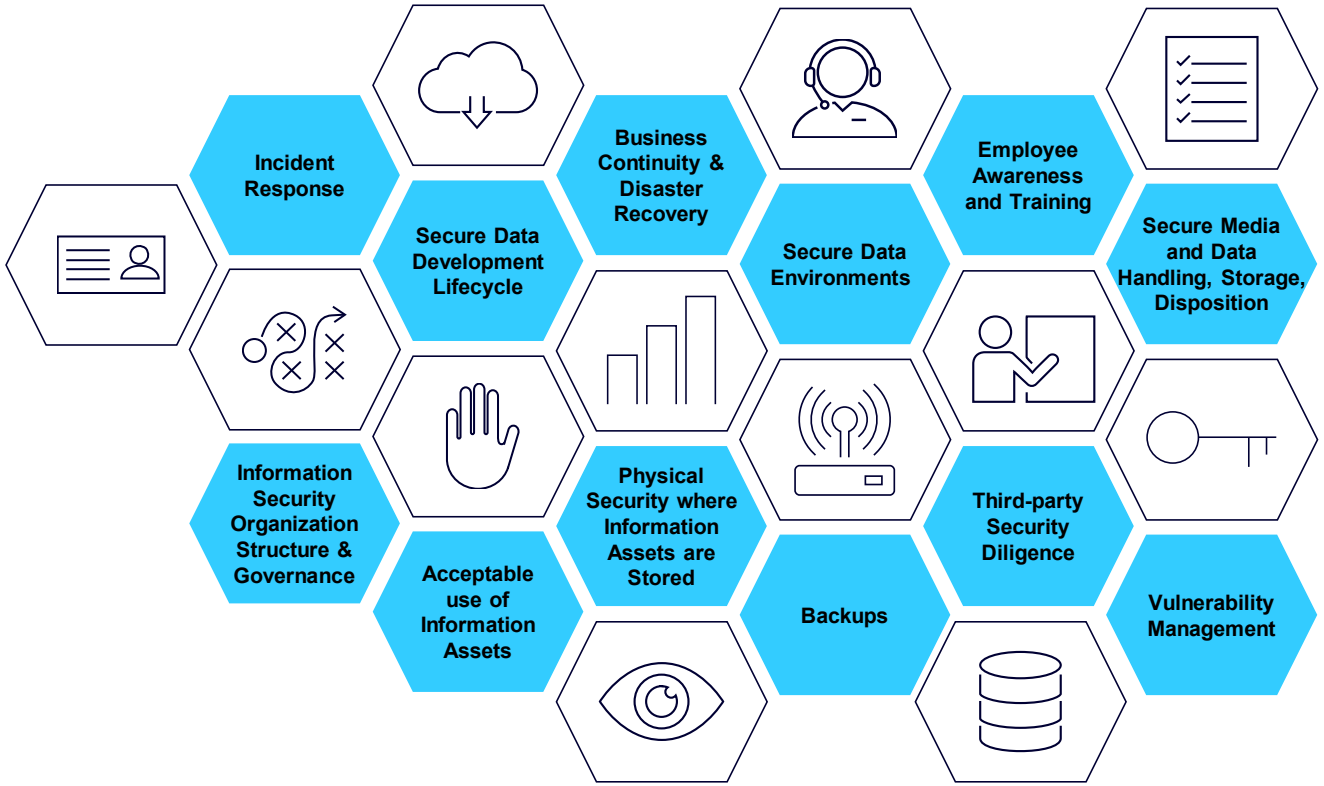
- Personal information about employees and customers;
- Nonpublic business information about, for example:
  - strategies, financial and contractual performance;
  - product plans and
  - strategies; and,
  - consultants, business partners, stakeholders and third-party suppliers.

The standards in the framework are reviewed by the information security team the sooner of either annually or whenever there is a significant change to Acumatica operations or legal or regulatory requirements warranting review.
New policies or modifications to existing policies are communicated to applicable employees. In addition, procedures are created and implemented to carry out the information security policies.

Information Security Management

SYSTEM

The Acumatica information security management system addresses, without limitation and solely for purposes of illustrating its *comprehensive scope*:



Information Security Management

OBJECTIVES

The *objectives* of the information security program are to:

- Reduce information security risks to an acceptable level.
- Ensure Acumatica assets are appropriately protected and yet remain available in line with the parameters of business requirements.
- Ensure Acumatica information shared with other parties is protected against unauthorized disclosure and is managed in compliance with internal policies.
- Ensure Acumatica personnel are aware of commitments and comply with applicable legislative and regulatory requirements.
- Maintain staff awareness of information security, thereby ensuring that all employees understand its importance to Acumatica and their own individual responsibilities for security.
- Ensure actual or potential breaches of information security are reported to and investigated by the IT Group who has direct responsibility for providing advice and guidance on policy implementation.
- Ensure information security controls are implemented to a repeatable and consistently high standard.
- Provide documented evidence to show processes are being followed correctly and completely.
- Continually improve the information security system based on customer and staff feedback, incidents, key performance indicator results, audit findings and new technologies.
- Enable the rapid dissemination of improvements to all relevant areas.

Information security objectives are formally reviewed annually as part of Acumatica's management review program. Key performance targets are identified and monitored, measured and reported at corporate, department and project levels as appropriate. Information security targets are:

- Detailed by key performance measures or achievable targets;
- Evaluated in annual risk assessments for effectiveness and efficiency; and,
- Reviewed by an information security forum and senior management to protect information assets from threats.

Illustrative Information Security Program (continued 1/4)

FOCAL POINTS

Acceptable Use

Acumatica maintains, monitors and enforces acceptable use policies for employee and contractor use of Internet, email, software, internal systems, portable and remote devices, instant messages and telephone equipment, and any other information asset.

Media & Information Handling

Acumatica requires assignment of labels to data and media, using classification schemes based on sensitivity. Retention and disposition of data and media is governed by legal and regulatory requirements, or, where none apply, by business and technical rationales including information security imperatives. Acumatica manages data and media according to pre-defined retention rules and destroys media and data in a secure manner when no longer needed. Data of a sensitive nature processed and transmitted by Acumatica uses appropriate cryptographic controls to maintain confidentiality and integrity.

Personnel Management

Acumatica conducts background reviews in compliance with applicable laws before hiring any job candidate and requires agreement to terms and conditions, including confidentiality and information security policies, in advance of commencement of employment duties. Employees are trained on security policies upon hire, as well as every subsequent year of employment. Acumatica maintains documented procedures to ensure that any changes to employment status include termination or change of access rights and return of company information assets.

Illustrative Information Security Program (continued 2/4)

Physical Security

Acumatica deploys security and access control mechanisms around all site perimeters, including exterior entrances and loading zones. Interior access is controlled by access control mechanisms, that may include using badge identification and access controls for authorization to controlled areas. Visitors are appropriately identified and their access appropriately limited. CCTV is used for certain facilities and areas where information assets reside.

Backups

Acumatica conducts regular backup of critical systems and data to ensure essential business information and software can be recovered in the event of a critical failure or natural disaster; backup processes include requirements for backup encryption, scheduling, and media handling.

Availability of customer data is ensured through a system of redundant backups across AWS regions, daily, weekly, monthly and quarterly. The backups are encrypted as well as regularly tested. Retention of the various backups is scheduled so as to provide for recovery under multiple different scenarios and varying historical timing implications.

Vulnerability Management

Acumatica deploys anti-malware protection to protect systems from malicious code. We have established controls to manage anti-malware software to provide up to date, real-time protection against threats. In addition, we regularly test our critical systems using scanning tools and penetration testing in order to actively discover new vulnerabilities. In order to minimize exposure to security flaws, all systems and hardware follow a patch management process to ensure software and operating systems are protected.

Illustrative Information Security Program (continued 3/4)

System & Network Management

Acumatica implements formal system acceptance, configuration, and hardening procedures for all servers, workstations and network hardware. Security controls are in place to manage external network connections and wireless networks, including appropriate security controls for mobile device use and telecommuters. An asset management system assigns ownership, labels and tracks Acumatica assets. Logging and alerts for potential security incidents at key information repositories or transit points is enabled and monitored.

Secure Data Environments

Acumatica segments internal networks to provide adequate security for confidential or restricted data. Zones are logically separated using network devices, with access to secure zones restricted by job function and business need.

Software Development

Acumatica's documented software development standards include processes for securely designing, developing, testing and implementing software. Development standards include details on developing software using security best practices in addition to testing for common security vulnerabilities. Appropriate separation of duties, as well as separate test environments is required for all development projects. Source code is secured so that it is only accessible by individuals with a legitimate business need for such access. Data used in testing is cleansed of sensitive information and test data removed before implementation.

Illustrative Information Security Program (continued 4/4)

Incident Handling

A comprehensive incident handling process is in place to respond to security breaches, fraud, faults and other disruptions to business processes, contractual agreements or privacy.

Third Parties

Acumatica requires third party service providers to undergo an approval process and monitors for compliance against information security and service delivery agreements. Any third party accessing Acumatica systems, including client service providers and contractors, are required to abide by applicable Acumatica security policies as well as any applicable legal and regulatory standards. Third parties with access to Acumatica systems must sign non-disclosure agreements. Acumatica data is exchanged with third parties only through a formal data exchange agreement process.

Personal Data Privacy

Employees and other individuals, who may have rights under data privacy regimes like the GDPR in the European Union, look to corporate custodians of digital information about them for effectuating their personal choices about how that data is collected and used. Acumatica's ERP solutions facilitate compliance with data subject rights through the protections afforded by the Acumatica information security program along with features, functionality and services like the access control options Acumatica provides. Acumatica provides customers with a clear path to data privacy compliance by prioritizing data privacy concerns in the design of our solutions.

IN SUMMARY

Information technology without information security is useless – it's an enterprise risk issue. As providers of ERP software and services, we do not control what data our customers import or how they manage access within their organizations. But we do know that our customers expect us to do our part to contribute to a secure ERP information eco-system for their enterprises by applying responsible information security practices. The foregoing is intended to give a taste of how we handle that responsibility and the value we place on doing our part to minimize information security risk.

If you have further questions about Acumatica solutions and security, please contact Acumatica's compliance team by phone or email:

1-888-288-8300 or
1 425 658 4919

privacy@acumatica.com