



Data Management Policies

Sage ERP Online



Table of Contents

1.0	Server Backup and Restore Policy.....	3
1.1	Objectives	3
1.2	Scope.....	3
1.3	Responsibilities	3
1.4	Policy	4
1.5	Policy Violation	5
1.6	Communication.....	5
1.7	Monitoring and Review	5
1.8	Terms and Definitions	5
2.0	Electronic Data Protection Policy.....	6
2.1	Overview.....	6
2.2	Purpose.....	6
2.3	Scope.....	6
2.4	Key Definitions.....	7
2.5	Policy	7
2.6	Exceptions.....	9
2.7	Roles and Responsibilities	9
2.8	Failure to Comply	11
2.9	Enforcement.....	11
3.0	Virus Protection Policy.....	12
3.1	Purpose.....	12
3.2	Scope.....	12
3.3	Policy	12
3.4	Exceptions.....	13
3.5	Failure to Comply	13
3.6	Enforcement.....	13
4.0	Patch Management Policy.....	14
4.1	Overview.....	14
4.2	Purpose.....	14
4.3	Scope.....	14
4.4	Whom Does This Policy Affect?	14
4.5	Key Definitions.....	14
4.6	Policy	15
4.7	Failure to Comply	18
4.8	Exceptions.....	18
4.9	Enforcement.....	18
5.0	Conclusion	18

1.0 Server Backup and Restore Policy

1.1 Objectives

- This policy supplements the Information Security Policy to ensure the confidentiality, integrity, and availability of Sage ERP Online information assets. This policy defines the principles for safeguarding availability of information by ensuring effective measurements of backup and restoration are in place.

1.2 Scope

- This policy applies to data that resides on Sage ERP Online North American servers. It does not cover end-user information that is saved on individual PCs, notebooks, PDAs, laptop computers, and other such devices.
- This policy applies to all Sage ERP Online North American business units and functions. It covers both primary and secondary Sage Information Systems managed data centers located on the East Coast and West Coast respectively, of the United States.
- Backups performed as part of this policy are not intended to serve as data archival or retention purposes. Any need for data retention or archiving needs should be considered outside of the normal backup processes. Backups performed in accordance with this policy will be generally deleted after 30 days. For more information on data retention, please refer to the Data Retention Policy.

1.3 Responsibilities

- The Backup and Restore Policy forms part of the overall Information Security Policy. The Sage team is responsible for providing Sage personnel with advice and guidance on the Backup and Restore Policy.
- It is the responsibility of server administrators to ensure that all new servers are added to the appropriate backup cycle.

1.4 Policy

- ✓ The backup requirements of Sage ERP Online information assets are determined by the Information Owner, in this case the Sage ERP Online Team. The decision is based on risk and business assessments. The specified backup requirements include the extent (for example, full or differential), frequency, method, backup location, and retention period.
- ✓ An inventory of backup requirements is maintained and regularly reviewed by the Information Owners.
- ✓ When deploying a new server, a full backup is performed, and the ability to restore from that backup is confirmed.
- ✓ All backup data is replicated from the secure facility on the east coast of the US to the secure datacenter on the west coast of the US.
- ✓ All backup data is protected against environmental risks such as fire and water
- ✓ Backup data is protected with the same operational logical and physical security controls as the production data in both facilities
- ✓ All access to backup data, storage media, storage locations, and management tools is restricted to authorized personnel only.
- ✓ All backup logs are maintained and monitored and the relevant Information Owner is notified of any exceptions.
- ✓ Backups are performed prior to any major or critical change to information, systems, or applications.
- ✓ The Information Owner is responsible for coordinating with Sage to ensure that all critical data is backed up.
- ✓ Procedures are in place for the Information Owner to submit a data restore request.

1.5 Policy Violation

- Personnel who violate the Information Security Policy will be referred to Human Resources and may be liable to disciplinary action up to and including termination of employment, as per Sage’s disciplinary policy. Contractors or temporary staff will be referred to their senior manager and may be liable to sanctions as per the terms and conditions of their contract.

1.6 Communication

- This Backup and Restore Policy will be available and circulated to all Sage Operation teams.

1.7 Monitoring and Review

- This policy is reviewed as part of an overall management review of the effectiveness of Sage’s Information Security Management. The policy will also be reviewed in response to significant changes due to security incidents and/or changes to organizational or technical infrastructure.

1.8 Terms and Definitions

Term	Definition
Associates	Sage employees, contractors, and consultants
Backup	The act of saving business data to an alternate media or location for the purpose of protecting it.
SLT	Senior Leadership Team
Information Owner	Sage ERP Online Team

2.0 Electronic Data Protection Policy

2.1 Overview

- All Sage ERP Online data is protected and reviewed on a periodic basis.

2.2 Purpose

- This policy is to manage and protect Sage ERP Online client data from security breaches. This policy also outlines the controls necessary for accessing that data. Data protection ensures that individual and corporate sensitive information is properly safeguarded from loss, damage, inappropriate access, and unauthorized disclosure or use.

2.3 Scope

- This policy applies to all Sage ERP Online units and functions. The data covered by this policy includes but is not limited to all electronic information, regardless of the system owner, found in:
 - ✓ Email.
 - ✓ Databases.
 - ✓ Applications.
 - ✓ Files stored on local hard drives.
 - ✓ Other data residing on a server or network location such as the i:\drive.

2.4 Key Definitions

- Definitions related to the Data Protection Policy are as follows:

TERM	DEFINITION
Criticality	Determines the importance of customers' data to sustain the ongoing operations of their business. Takes into consideration a combination of confidentiality, availability, and integrity when referring to the data.
Sensitivity	The degree of susceptibility of the data. This drives what steps the Information Owner must take to prevent unauthorized access and modifications.
Least Privileges	Granting the minimum possible privileges to online customers, permit a legitimate action in order to enhance protection of data and functionality from faults and malicious behavior.

Table 1: Key Definitions—Data Protection Policy

2.5 Policy

- ✓ All Sage ERP Online information resources are categorized and protected. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the company. Users shall be granted the “least privileges” necessary to accomplish their tasks.
- ✓ Applications that need a certain level of access to run certain processes that do not directly involve a user such as nightly batch jobs shall be granted the “least privileges” necessary to perform their functions.
- ✓ General support systems shall be granted the “least privileges” necessary to fulfill their role in a larger network.
- ✓ A delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes is established, in the event that granular access cannot be granted, by granting the most restrictive access.
- ✓ No Sage ERP Online system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification. (Sage controls access to all external network connections, such as the Internet, point to point, and so on.)

- ✓ Any Sage ERP Online data (that is permissible for download) downloaded to a hard drive on a personal machine will be deleted once the associate is finished with the business task requiring the data. The associate is responsible for ensuring the data is deleted for data protection, security, and retention purposes.
- ✓ Sage is responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- ✓ All data will be backed up according to the classification level and the backups tested periodically as part of a documented, regular process.
- ✓ Backups of data are handled with the same security precautions as the data itself. Backups will only be stored in a Sage data center in a Sage-approved and -certified offsite media storage vendor location. Refer to the Server Backup Policy form more information on backups and refer to the Physical Access Control Policy for more information on Sage data centers and certified vendor location security precautions.
- ✓ Data server and backup storage facilities (whether on-site or off-site) will follow these minimum standards:
 - Storage facility is specifically designed to store, protect, and secure electronic data on various media
 - Free access to the facility will be limited to Sage data custodians
 - All Sage data custodians as well as any members of the Sage ERP Online Team members will have their individual or group access credentials to systems and facilities, removed, upon leaving Sage.
 - For approved vendor facilities, vendor access will be limited to those resources servicing the Sage ERP Online facility while Sage ERP Online media will be in a segregated, locked area, dedicated to Sage ERP Online resources
 - Escorted access to the facility will be limited to Sage approved personal and IT contractors
 - All resources entering the facility will be required to sign in and record purpose of visit, entrance time, and exit time
 - All approved vendors upon completion of their contracts with Sage will have their individual or group access credentials to systems and facilities, removed.
 - Facility will have adequate fire protection and inclement weather protection

- End user backups must be handled with the same security as the data itself; refer to the End User Backup Policy for more information on end-user backups
- ✓ When systems are disposed of or repurposed, data must be certified deleted or media destroyed consistent with NIST Special Publication 800-88 for the security level of the data. The specific method of sanitization will be chosen by Sage based on the Media Sanitization Decision Matrix in NIST Special Publication 800-88. The confidentiality level of the data on the media will be balanced with the cost of sanitization when the specific sanitization method (clear options, purge options, physical destruction options) is chosen.
- ✓ Sage may delegate the responsibility of the changing of access rights on systems (for example, a user making calendar data accessible) but ultimately remains responsible for the control and audit of such changes.

2.6 Exceptions

- Exceptions to this policy are not permitted. No other variants are permitted without the express written consent of two SLT members.

2.7 Roles and Responsibilities

- A description of the Roles and Responsibilities necessary to comply with the Data Protection Policy is as follows:

ROLE	DESCRIPTION
Business Owner	<ul style="list-style-type: none"> ▪ Responsible for fiscally funding Sage to ensure data is adequately protected on Sage ERP Online systems.
Data Owner	<ul style="list-style-type: none"> ▪ Verifies that only authorized users have access to information data. ▪ Classifies data, notifies IS representative of classification levels, and reports any changes of classification to the designated IS representative. ▪ Obligated to notify IS about “least privileges.” ▪ Ensures that the data is protected in a manner appropriate to its classification ▪ May enact more restrictive policies for end-user access to their data. ▪ Responsible for determining what data access rights should be.

ROLE	DESCRIPTION
Application Developer/Database Administrator	<ul style="list-style-type: none"> ▪ Implements and monitors approved access control solutions on computer systems. ▪ Ensures that all sensitive applications have the appropriate audit functions to abide by state, local, and federal laws.
Sage	<ul style="list-style-type: none"> ▪ Prevents unauthorized access to information data. ▪ Adheres to “least privileges” of sensitive information to ensure the confidentiality, integrity, and authorization of that information. ▪ Ensures that appropriate data authentication is designed to combat fraud and makes the Sage network more secure. ▪ Ensures that every program or system component will operate with the minimum set of privileges it needs to accomplish its task. ▪ Responsible for protecting data residing on IS systems as specified by the data owner.

Table 2: Roles and Responsibilities—Data Protection Policy

2.8 Failure to Comply

- Failure to comply with this policy will result in disciplinary action, depending on the sensitivity of the transgression.

2.9 Enforcement

- Both automated systems and manual processes will be used to make routine audits to enforce the Data Protection policy. Individuals seeking employment at Sage are required to sign the Sage Software, Inc. Privacy Statement Acknowledgement and Employee Agreement provided by the Human Resources Department.

3.0 Virus Protection Policy

3.1 Purpose

- Malicious software are actively guarded against within the Sage ERP Online network. This policy is designed to protect organizational computing resources against infection by viruses and other malware.

3.2 Scope

- This policy applies to all computers that are connected to the Sage ERP Online production network through standard network connections, or virtual private network (VPN) connections. This policy includes computers owned by Sage and computing devices owned by individuals that attach to the Sage ERP Online network.

3.3 Policy

- All computers attached to the Sage ERP Online production network have standard, Sage supported antivirus software installed. This software must be active, be scheduled to perform malware checks at regular intervals, and have its malware definition files updated at least once per day.
- Antivirus software for machines connected to the Sage ERP Online production network should be administered solely by Sage.
- The settings for the virus protection software are not to be altered in a manner that will reduce the effectiveness of the software. Tampering with the settings of the antivirus software (including disabling certain features such as active malware scanning) is a violation of this policy.
- Sage reserves the right to filter email attachments, especially those that have a higher connection to viruses.
- Any computer that cannot have the approved antivirus software loaded and actively running must never be connected to the Sage ERP Online network.
- Any activities with the intention to create and/or distribute malicious programs onto the Sage ERP Online network for example, viruses, worms, Trojan horses, email bombs, and so on is strictly prohibited.
- If an associate receives what he/she believes to be a virus, spyware, or other malware, or suspects that a computer is infected with malware, it must be reported immediately to the Service Desk with the following information (if known): malware name, extent of infection, source of malware, and potential recipients of infected material. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the North American Service Desk.

- Any malware-infected computer will be removed or segmented from the network until it is verified as malware-free.

3.4 Exceptions

- Exceptions to this policy must be approved by the Sage leaders.

3.5 Failure to Comply

- Failure to comply with this policy will result in disciplinary action up to and including termination of employment, services, or relationship with Sage North America. In addition, Sage reserves the right to confiscate and/or remove from the network any equipment not in compliance with this policy. This may be done with or without notice to the owner of the equipment.

3.6 Enforcement

- Periodic scans of network-connected devices will be conducted by Sage to ensure compliance. In addition, the source of any malware found on the network will be thoroughly investigated and analyzed. If the source of the problem is found to be in violation of this policy then the appropriate disciplinary action will be taken and the violating equipment or application (if applicable) may be removed from the network.

4.0 Patch Management Policy

4.1 Overview

- Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations and place the integrity of data maintained by Sage ERP Online at risk. Patches are additional pieces of code developed to enable additional functionality or address security flaws within a program.

4.2 Purpose

- The purpose of this policy is to ensure computer systems attached to the Sage ERP Online network infrastructure are updated accurately and in a timely manner with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

4.3 Scope

- This policy applies to all North American business units and functions. It covers all equipment located in a Sage facility or otherwise connected to the Sage network regardless of which group manages the equipment. It also covers systems that are managed by Sage employees that are not connected to the Sage network if these assets store, transmit, or process Sage data (for example, systems hosted by third parties but managed by Sage employees).

4.4 Whom Does This Policy Affect?

- All Sage ERP Online associates.

4.5 Key Definitions

- Definitions related to the Patch Management Policy are as follows:

TERM	DEFINITION
Patch	The most up-to-date virus protection software, current virus definition libraries, and the most recent operating system and security upgrades to computing resources.
SLT	The leadership team of the North American Sage organization.
Vulnerability	A weakness in a system that allows an attacker to violate the integrity of that system.

TERM	DEFINITION
Exploit	An exploit is a piece of software, group of data, or sequence of commands that take advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware.
IDS	An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Table 3: Key Definitions—Patch Management Policy

4.6 Policy

Monitoring

The Sage Security Team will monitor security mailing lists, review vendor notifications and websites, and research specific public websites for the release of new patches. Monitoring will include, but not be limited to, the following:

- Monitoring CERT, notifications, and websites of all vendors that have hardware or software operating on the Sage ERP Online network.
- Scanning Sage ERP Online network to identify known vulnerabilities.
- Identifying and communicating identified vulnerabilities and/or security breaches to Sage’s Chief Information Security Officer.

Review and evaluation

- Once alerted to a new patch, the Sage Security Team will review the new patch within 1 (one) business day of its release. The Security Team will determine if a patch is applicable and categorize the criticality of the patch
- Regardless of platform or criticality, all patch releases will follow a defined policy for patch deployment that includes assessing the risk, testing (where applicable), scheduling, installing, and verifying. Administrators must apply all system and security patches in accordance with the schedule above after they have been tested and approved.

Risk assessment and testing

- Sage will assess the effect of a patch on the Sage ERP Online infrastructure prior to its deployment. Sage will also assess the affected

patch for criticality relevant to each platform (for example, servers, desktops, and so on). Software updates and patches must be researched, tested, and verified by appropriate personnel before installing on any Sage ERP Online asset.

- If Sage categorizes a patch as Critical, the department considers it an imminent threat to the Sage ERP Online network. Therefore, Sage ERP Online assumes greater risk by not implementing the patch than waiting to test it before implementing.
- All non-Critical patches will undergo testing for each affected platform before release for implementation. Sage will expedite testing for patches rated High. The department must complete validation against all images (for example, Windows, VMs, and more) prior to implementation.

Notification and scheduling

- The management staff of the designated teams responsible for patch management must approve the schedule prior to implementation. Except for Critical patches, each patch release requires the creation and approval of a Request For Change (RFC) through the Operational Change Management process prior to releasing the patch for implementation. The Sage Security Team may approve the release of Critical patches without approval of a RFC; however, the RFC must be filled out post deployment to comply with the Operational Change Management process.

Implementation

- Sage will begin deployment of Critical patches within three business days of availability. As Critical patches pose an imminent threat to the network, in some instances the release may precede testing. In all instances, the group will perform testing (either pre- or post-implementation) and document it for auditing and tracking purposes.
- Except for patches classified as Critical, each patch or group of patches will require an approved RFC. Sage will obtain authorization for implementing Critical patches through an emergency RCF approval. The department will implement non-Critical patches during regularly scheduled preventative maintenance.
- For new network devices, each platform will follow established hardening procedures to ensure the installation of the most recent patches.
- All systems specified in the scope section of this document must comply with this policy even if Sage does not directly manage the system.

Auditing, assessment, and verification

- Following the release of all patches, Sage staff will verify the successful installation of the patch and that there have been no adverse effects.

4.7 Failure to Comply

- Failure to comply with this policy will result in disciplinary action. In addition, any servers not in compliance with this policy may be confiscated by Sage.
- Any exceptions to this policy must be approved in advance by both the Information Security Officer and the Chief Information Officer.

4.8 Exceptions

- Systems that are separated from the Sage ERP Online network through the use of a Sage managed firewall may be exempt from the patching policy if the systems have been identified as noncritical, do not handle sensitive data, and are explicitly identified as belonging in a security zone that does not require patching.
- All other exceptions require the explicit written consent of the Sage security manager.

4.9 Enforcement

- Both automated systems and manual processes will be used to perform routine audits in an effort of enforcing the Patch Management Policy.

5.0 Conclusion

As market and industry conditions change, this document will be reviewed and updated at least yearly. Sage reserves all rights to make changes to this document at its sole discretion.

Published: 7 October 2011