Softdocs

# SECURITY COMPLIANCE POLICY AND PROCEDURES

Shared Responsibilites Model

# TABLE OF CONTENTS

# Shared Responsibilities Model

## 1.0 Purpose

The purpose of this document is to define the Softdocs Cloud Shared Responsibilities Model to be agreed upon by customers utilizing Softdoc's Cloud offering. Your organization may have licensed some or all of the products and solutions detailed in this document. A Shared Responsibility Model outlines the responsibilities of both cloud providers and customer in securing cloud resources and data. This policy is crucial for ensuring that all parties involved understand their respective obligations and can work together effectively to maintain security.

## 2.0 Cloud Shared Responsibilities

In a shared responsibility model, a layered approach to security is taken:

- For on-premises solutions, the customer is responsible for all aspects of security and operations.
- For a Cloud Solution, Softdocs provides the application and underlying technologies. The customer continues to be accountable; they must ensure that data is classified correctly, and they share a responsibility to manage their users and devices.
- The importance of understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts. Still, these advantages do not absolve the customer of the responsibility to act to protect their data, users, applications, and service offerings.

## 3.0 Customer Responsibilities

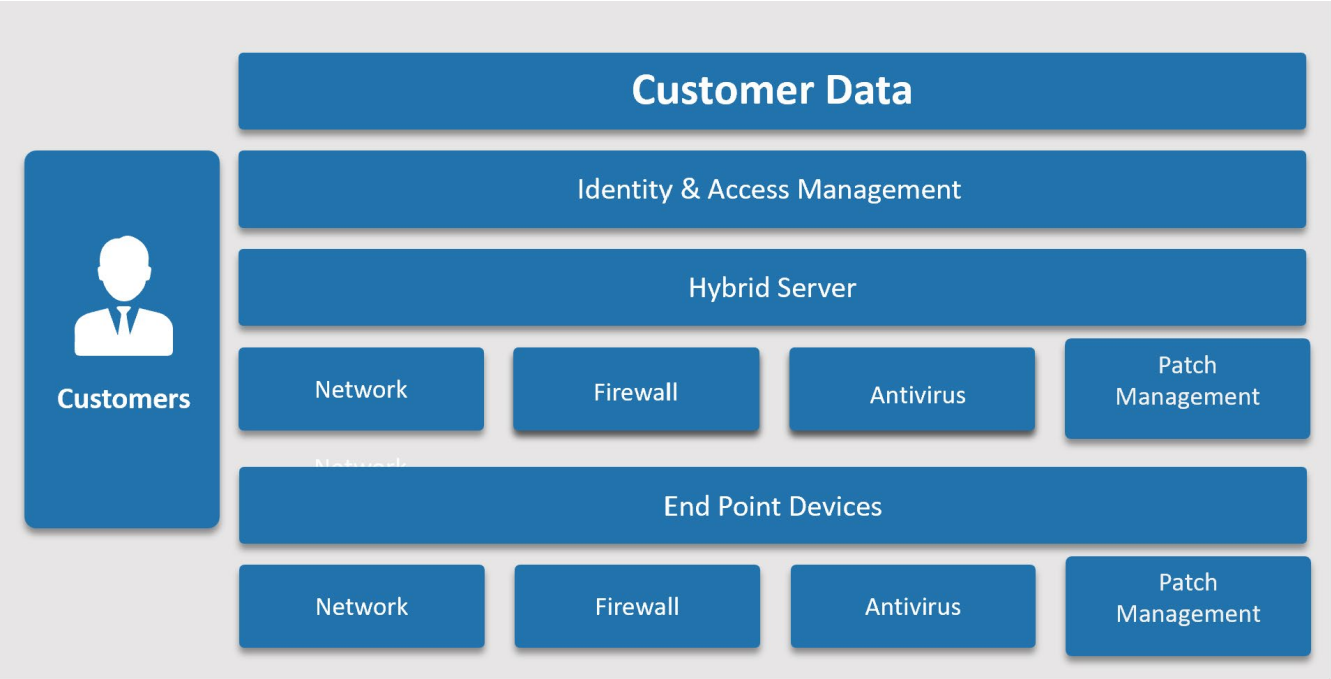
Customers are responsible for these primary areas regarding their Cloud deployment:

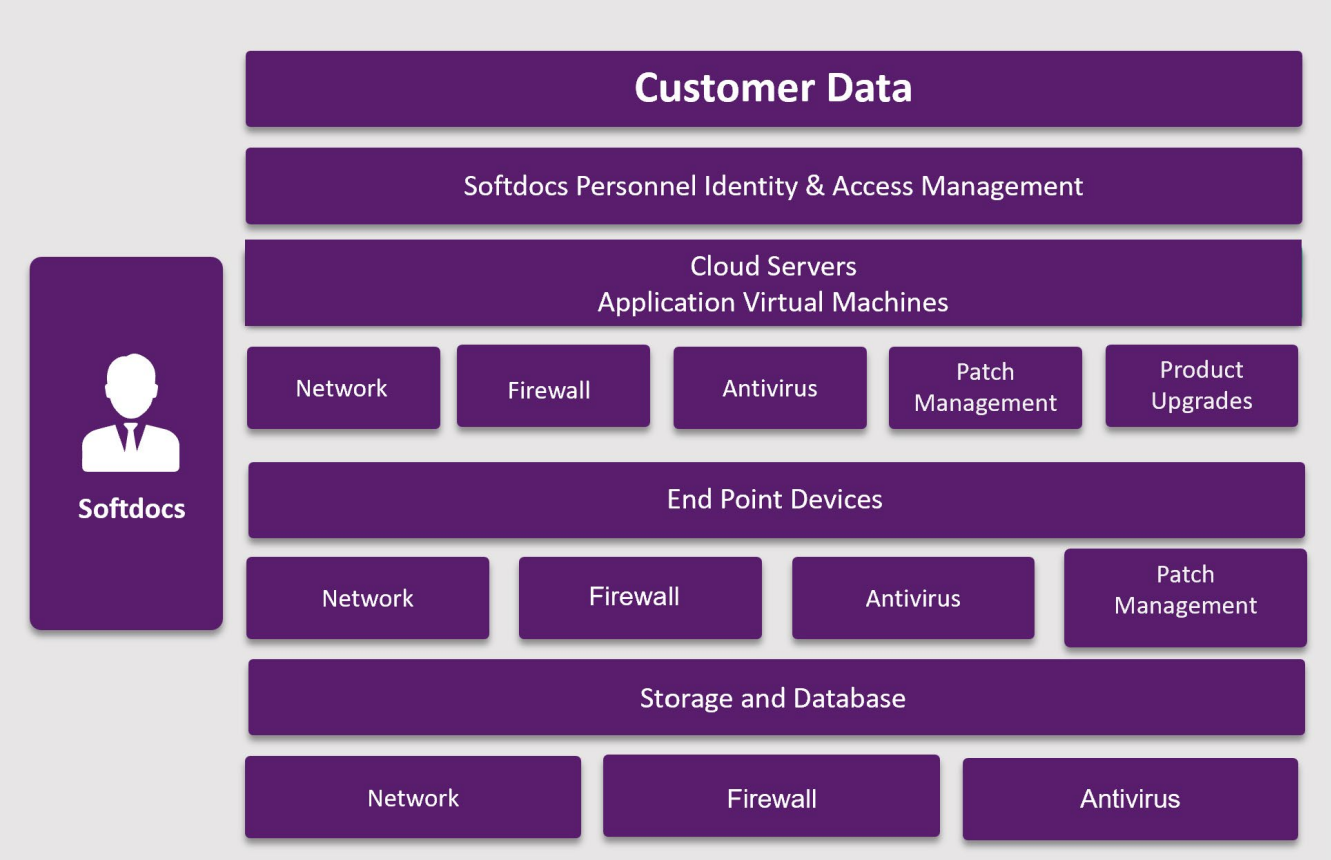
- **User Hardware:** Customers provide the user-side hardware and operating environments, including desktop workstations, mobile devices, and scanners required to interact with the resources located in the data center.
- **Identity and Access Management (IAM):** Customers manage user access and authentication. This includes auditing the account creation, modification, enabling, disabling, and removal actions and deactivating users after an inactivity period.
- **Hybrid Server:** Customers provide and are responsible for the hardware and maintenance of the server. This includes network, local databases, patch management, firewall, and antivirus. The customer is responsible for backing up this server on their scheduled backup policies.
- **Replicated Reporting Database of Etrieve:** If a customer licenses the Replicated Reporting Database for Etrieve, the customer acknowledges that production data contains PII and should be safeguarded and secured on the hybrid server.
- **Data:** Customers own and are responsible for their data. Data classification is the responsibility of our customers. Additionally, customers are responsible for their data retention policies and the purge or archival of data.
- **Network Connection:** Customers must provide a network connection via the Internet, VPN or private line to the primary data center(s) in which their solutions are deployed. Deployments based on certain

scripted or advanced communications methods between Softdocs products and other customer applications may require private-line or VPN connectivity.

- **Coordinator:** Depending on the specific site configuration, customers are responsible for designating one or more coordinators to work with the Cloud Operations team.
    - The coordinator is:
        - required to attend product training.
        - the primary organizer of customer resources involved with deployment planning and assurance.
        - the point of contact for the technology rollout and ongoing maintenance or administration of the Etrieve application.

## 4.0 Overview of Responsibilities



## 5.0 Revision History

| Revision #: | Document History & Revision Summay | Author | Date |
|---|---|---|---|
| 1.0 | Initial Draft | Steve Johnston | 06/01/2018 |
| 1.1 | Content and Format updates | Steve Johnston | 06/05/2018 |
| 2.0 | Reviewed and approved. | Terri McKinney | 07/17/2020 |
| 3.0 | Policy reviewed and approved. | Terri McKinney | 06/16/2021 |
| 4.0 | Policy review and approved. | Terri McKinney | 06/16/2022 |
| 5.0 | Policy review | Alan Atkins | 03/23/2023 |
| 6.0 | Added approval history. | Terri McKinney | 03/23/2023 |
| 7.0 | Incorporated additional details for purpose. Added IAM, Hybrid Server, and Data details to Section 3. | Terri McKinney | 09/28/2023 |
| 7.1 | Security Team reviewed and approved. | Security Team | 10/23/2023 |
| 8.0 | Added visual representation of shared responsibilities. | Terri McKinney | 10/31/2023 |
| 9.0 | Added improvements to Section 2 based on Billy's recommendations | Terri McKinney | 02/22/2024 |

## 6.0 Approval History

| Revision #: | Approval Notes | Approval By: | Date |
|---|---|---|---|
| 6.0 | Policy reviewed and approved. | Terri McKinney | 03/23/2023 |
| 8.0 | Policy reviewed and approved. | Terri McKinney | 10/31/2023 |
| 9.0 | Policy reviewed and approved. | Terri McKinney | 02/22/2024 |