



**A-LIGN**

A-LIGN.com

# Type 2 SOC 3

Prepared for:  
KnowBe4, Inc.

Year:  
2026

**KnowBe4**  
Human error. Conquered.

**SOC 3 FOR SERVICE ORGANIZATIONS REPORT**

**March 16, 2025 to March 15, 2026**

## Table of Contents

<b>SECTION 1 ASSERTION OF KNOWBE4, INC. MANAGEMENT</b> .....	<b>1</b>
<b>SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT</b> .....	<b>3</b>
<b>SECTION 3 KNOWBE4, INC.’S DESCRIPTION OF ITS CLOUD HOSTED DATA PLATFORMS SYSTEM THROUGHOUT THE PERIOD MARCH 16, 2025 TO MARCH 15, 2026</b> .....	<b>6</b>
OVERVIEW OF OPERATIONS.....	7
Company Background .....	7
Description of Services Provided .....	7
Principal Service Commitments and System Requirements.....	11
Components of the System.....	12
Boundaries of the System.....	19
Changes to the System Since the Last Review.....	19
Incidents Since the Last Review .....	19
Criteria Not Applicable to the System .....	19
Subservice Organizations.....	20
COMPLEMENTARY USER ENTITY CONTROLS.....	22

**SECTION 1**  
**ASSERTION OF KNOWBE4, INC. MANAGEMENT**

## ASSERTION OF KNOWBE4, INC. MANAGEMENT

May 1, 2026

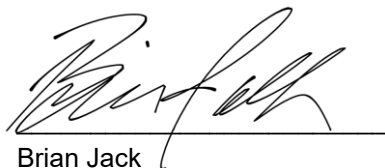
We are responsible for designing, implementing, operating, and maintaining effective controls within KnowBe4, Inc.'s ('KnowBe4' or 'the Company') Cloud Hosted Data Platforms System throughout the period March 16, 2025 to March 15, 2026, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*, and KnowBe4's compliance with the commitments in its Privacy Notice. Our description of the boundaries of the system is presented below in "KnowBe4, Inc.'s Description of Its Cloud Hosted Data Platforms System throughout the period March 16, 2025 to March 15, 2026" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 16, 2025 to March 15, 2026, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the trust services criteria. KnowBe4's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "KnowBe4, Inc.'s Description of Its Cloud Hosted Data Platforms System throughout the period March 16, 2025 to March 15, 2026".

KnowBe4 uses Amazon Web Services ('AWS') and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at KnowBe4, to achieve KnowBe4's service commitments and system requirements based on the applicable trust services criteria and KnowBe4's compliance with the commitments in its Privacy Notice. The description presents KnowBe4's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of KnowBe4's controls. The description does not disclose the actual controls at the subservice organizations.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 16, 2025 to March 15, 2026 to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the applicable trust services criteria and KnowBe4's compliance with the commitments in its Privacy Notice, if complementary subservice organization controls assumed in the design of KnowBe4's controls operated effectively throughout that period.



Brian Jack  
CISO  
KnowBe4, Inc.

**SECTION 2**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT

To: KnowBe4, Inc.

### *Subject*

We have examined KnowBe4's accompanying assertion titled "Assertion of KnowBe4, Inc. Management" (assertion) that the controls within KnowBe4's Cloud Hosted Data Platforms System were effective throughout the period March 16, 2025 to March 15, 2026, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, and KnowBe4's compliance with the commitments in its Privacy Notice.

KnowBe4 uses AWS and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at KnowBe4, to achieve KnowBe4's service commitments and system requirements based on the applicable trust services criteria and KnowBe4's compliance with the commitments in its Privacy Notice. The description presents KnowBe4's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of KnowBe4's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

### *Service Organization's Responsibilities*

KnowBe4 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved. KnowBe4 has also provided the accompanying assertion (KnowBe4 assertion) about the effectiveness of controls within the system. When preparing its assertion, KnowBe4 is responsible for selecting, and identifying in its assertion, the applicable trust services criteria, for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system, and complying with the commitments in its Privacy Notice.

### *Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and its compliance with the commitments in its Privacy Notice. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

#### *Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

#### *Inherent Limitations*

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

#### *Opinion*

In our opinion, management's assertion that the controls within KnowBe4's Cloud Hosted Data Platforms System were suitably designed and operating effectively throughout the period March 16, 2025 to March 15, 2026, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls assumed in the design of KnowBe4's controls operated effectively throughout that period.

The SOC logo for Service Organizations on KnowBe4's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

#### *Restricted Use*

This report, is intended solely for the information and use of KnowBe4, user entities of KnowBe4's Cloud Hosted Data Platforms during some or all of the period March 16, 2025 to March 15, 2026, business partners of KnowBe4 subject to risks arising from interactions with the Cloud Hosted Data Platforms, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida  
May 1, 2026

**SECTION 3**

**KNOWBE4, INC.'S DESCRIPTION OF ITS CLOUD HOSTED DATA PLATFORMS  
SYSTEM THROUGHOUT THE PERIOD MARCH 16, 2025  
TO MARCH 15, 2026**

## OVERVIEW OF OPERATIONS

### Company Background

KnowBe4 is the world's first and largest new-school security awareness training and simulated phishing platform (KSAT); lightweight security orchestration, automation, and response platform (PhishER), along with SecurityCoach which is a real-time security coaching aimed at reducing risky behavior utilizing Human Detection and Response (HDR) techniques to correlate events from existing security infrastructure. Founded by data and Information Technology (IT) security expert Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness of risks such as ransomware, Chief Executive Officer (CEO) fraud, and other social engineering tactics through a new-school approach to security awareness training. Thousands of organizations leverage KnowBe4's platform to train their workforce to make smarter security decisions and create a human firewall.

In 2024, KnowBe4 acquired Egress Software Technologies Ltd (becoming Egress, a KnowBe4 Company, or "Egress"), and introduced the Protect, Defend, and Prevent ("PDP") products into the KnowBe4 suite.

### Description of Services Provided

KnowBe4's Security Awareness Training and Simulated Phishing (KSAT) is designed to provide users with a platform to better manage IT security problems of social engineering, spear-phishing, and ransomware attacks.

The KSAT platform provides users with self-service enrollment and both pre-and post-training phishing security tests that show the percentage of end-users that are Phish-prone. KnowBe4's random Phishing Security Tests provide several remedial options if an employee falls for a simulated phishing attack. The KSAT platform is a comprehensive web-based Software as a Service (SaaS) service designed to help organizations manage the ongoing problem of social engineering.

KSAT provides access to the world's largest library of security awareness training content, including interactive modules, videos, games, posters, newsletters, and compliance training. The platform simulates phishing attacks to test employees' vigilance and train them to recognize and report attempts. Phish Alert Button (PAB) enables users to report suspected phishing e-mails with a single click. KSAT offers advanced reporting features that provide insights into the effectiveness of the training programs and the phish-prone percentage of users. The smart group's feature allows for the tailoring of phishing campaigns, training assignments, remedial learning, and reporting. KSAT can synchronize with an organization's Active Directory (AD). Security Roles for granular access control for different users and groups. The KSAT platform is designed to be intuitive and easy to use, allowing for quick deployment and management of training and phishing campaigns.

KSAT platform's key features:

- User Management and Reporting:
  - Easy User Management with AD Integration
  - SmartGroups to automate user training paths based on behavior and user attributes
  - Granular Security Roles for access control within the console
  - Enterprise-Strength Reporting for actionable metrics on security awareness program
- Phishing Simulation Features:
  - Phishing Templates available in over 30 languages
  - Artificial Intelligence (AI) Based Phishing for dynamic and adaptive phishing tests
  - Domain Spoofing capabilities for realistic simulations
  - Randomized Testing to prevent pattern recognition among users
  - Full Customization of phishing templates and landing pages
  - Over 20,000 templates to choose from, fully localized

- Training Campaign Options:
  - Configurable Start Times and Time zones
  - Business Hours option to send phishing tests within work hours
  - Frequency and Duration settings for campaign customization
  - Target Specific Groups or users with campaigns
- Phish Alert Button (PAB):
  - Functionality for users to report phishing attempts
  - Data Capture details available in the Product Manual
  - Environment Customization for the Phish Alert Button
- Advanced Phishing Features:
  - Phishing Reply Tracking to monitor user responses to simulated phishing e-mails
  - Geolocation data to visualize phishing test failures
  - Social Engineering Indicators to educate users on phishing e-mails
  - USB Drive Test to assess user reactions to unknown USB drives
- Training Access Levels:
  - Multiple levels of access to a vast content library based on subscription levels
  - Always-fresh content to address the needs of any organization size
- Additional Features:
  - Advanced Reporting with over 60 built-in reports
  - Unlimited Use of phishing features and access to the content library
  - Simulated Attachments in various file formats for phishing tests
  - Risk Scoring to monitor the risk level of employees and groups
- Integrations:
  - AD and Security Assertion Markup Language (SAML) Integration for user synchronization and single sign-on
  - Various third-party integrations to enhance functionality and data analysis
- Automated Security Awareness Program (ASAP):
  - ASAP is a tool that allows the creation of a customized Security Awareness Program to create a fully mature training program

PhishER is KnowBe4's lightweight Security Orchestration, Automation, and Response (SOAR) platform designed to help manage e-mails reported by users as suspicious.

It's an integral part of a security incident response plan, providing a centralized platform to help prioritize and analyze these reported messages. The purpose of this platform is to provide an organization with a way to evaluate suspicious e-mails making it through to the inbox of users. Using PhishER as a detective security control, the organization can identify potential threats and strengthen its security measures and defense-in-depth plan.

PhishER's key features:

- Simple and Advanced Rule Creation: PhishER allows the creation of custom rules using a Basic or Advanced Editor, utilizing built-in YARA-based system rules, or editing existing YARA rules to disposition and categorize messages efficiently.?
- PhishML: A machine-learning module within PhishER that helps to identify and assess the potential threat of suspicious messages reported by users. It generates confidence values and allows users to customize threshold values for automated prioritization.
- Data Enrichment and Intelligence: PhishER can integrate with external services like VirusTotal to analyze attachments and URLs for malicious content, providing additional context and intelligence for reported messages.
- Security information and event management (SIEM) Integrations: PhishER can connect with existing security infrastructure to maximize customers security investments and streamline incident response.
- PhishRIP: An e-mail quarantine feature that integrates with Microsoft 365 and Google Workspace, allows the search for and removes threats across mailboxes.

- Automatic Message Prioritization: PhishER automatically prioritizes every reported message into one of three categories: Clean, Spam, or Threat, helping the team focus on the most dangerous threats first.
- PhishFlip: This feature allows for turning user-reported phishing attacks targeted at customer organizations into safe simulated phishing campaigns, enhancing customer training programs.
- Emergency Rooms: These are pre-filtered views of unresolved messages in the PhishER inbox, grouped by commonalities, which help to quickly address potential threats.

AIDA (Artificial Intelligence Defense Agents), is a suite of agents that up-levels the approach to human risk management by leveraging multiple AI technologies to create personalized, adaptive, and highly effective training for users that actually changes behavior. AIDA helps significantly reduce human risk, streamline security operations, and support a strong security culture that meets the challenges of a rapidly escalating threat landscape.

#### AIDA Features:

- Automated Training Agent
- Template Generation Agent
- Knowledge Refresher Agent
- Policy Quiz Agent

SecurityCoach allows the Security team to leverage existing cybersecurity infrastructure to identify risky user behaviors. SecurityCoach then helps to augment the security awareness training effectiveness with a data-driven approach by quantifying and reducing human risk with real-time behavior coaching and new school security awareness training.

SecurityCoach is an add-on for KnowBe4's Platinum and Diamond customers that enhances the security awareness training experience by providing real-time coaching based on user behavior. It integrates with customer security stack to detect and address risky user behavior as it occurs, reinforcing a robust security culture within customer organization.

#### SecurityCoach Key features:

- Real-Time Coaching: SecurityCoach monitors user activity for risky behavior and delivers instant, automated SecurityTips to coach users on safer practices. This real-time feedback helps correct actions that could lead to security incidents.
- Vendor Integrations: The platform integrates with various third-party security vendors to leverage data for user coaching. This integration allows SecurityCoach to use events detected by existing security solutions to provide targeted coaching.
- User Mapping: SecurityCoach links risky activity detected by security vendors to specific users, enabling personalized coaching. This mapping can be done automatically for e-mail and web security vendors and either manually or automatically for endpoint security vendors.
- Detection Rules: The platform comes with system detection rules provided by KnowBe4 and also allows for the creation of custom rules. These rules are used to identify risky behavior and trigger real-time coaching.
- SecurityTips: These are customizable graphics and notification templates used in coaching campaigns. They can be filtered by type, topic, and language, and are designed to engage users and reinforce security best practices.
- Real-Time Coaching Campaigns: Training campaigns can be created to send SecurityTips when risky behavior is detected. These campaigns can be tested with specific user groups before rolling out organization wide.
- Dashboard and Reporting: SecurityCoach provides a comprehensive dashboard and reporting features that offer an overview of SecurityCoach data, risk reports for security vendors, detection rules reports, real-time coaching reports and vendor events reports.
- Workflow: The workflow of SecurityCoach involves third-party vendors monitoring for risky activity, sharing events with SecurityCoach, triggering detection rules, and sending SecurityTips if part of a campaign.

- Availability: SecurityCoach is available to Platinum and Diamond customers of KnowBe4, providing an additional layer of security awareness and behavior modification to complement the existing training and phishing simulation features.

KnowBe4 Prevent is an AI-driven e-mail security tool designed to help manage the problem of outbound e-mail risks head-on. Alongside its AI model, Prevent uses advanced machine learning to analyze e-mails in real-time, focusing on sender behavior, content, and recipients.

Prevent Enterprise includes additional features to tailor Prevent to organization's specific needs, like misdirected content detection, custom Data Loss Prevention (DLP) policies and integration with Microsoft Azure Information Protection (Purview).

#### Prevent Features:

- Misdirected E-mail Prevention
- Mistyped E-mail Address Detection
- Large Recipient List Protection (BCC)
- Multiple External Domain Monitoring
- First-Time Recipient Alerting
- E-mail Greeting Mismatch Detection
- Misdirected Content
- Data Exfiltration Prevention
- DLP Rule Enforcement
- Newly Registered Domain Monitoring
- Potential Impersonation Detection
- Malicious Domain Blocking
- Integration with Microsoft 365
- Detailed Analytics

KnowBe4 Defend is the adaptive anti-phishing technology designed to complement PhishER. By combining AI-powered detection, real-time user education, and actionable insights, Defend protects against today's sophisticated phishing threats while strengthening the organization's overall security posture.

#### Strategic Microsoft 365 Integration:

- Direct quarantine integration with Microsoft Defender for Office 365
- Complementary AI detection enhances Microsoft's native protections
- Unified management interface allows security teams to view KnowBe4 threat detections directly within their Microsoft console
- Seamless workflows maintain existing security investments
- Defend Features:
  - AI-enabled phishing detection
  - Adaptive security architecture
  - Contextual warning banners
  - Sender analysis
  - Link rewriting
  - QR code detection
  - Intelligent graymail detection
- Integration with Microsoft 365
- Integration with Microsoft Defender for Office 365
- Detailed analytics
- Single Sign On (SSO) enabled
- Integration with other security tools

Alongside Prevent and Defend is Protect, which offers the option for secure e-mail encryption at both the desktop or the e-mail gateway, and controls access to messages in shared mailboxes. It has full integration with Microsoft Outlook and Microsoft 365, allowing customers to secure and share data easily. There is also a mobile application which allows users to view and send encrypted e-mails.

Protect features:

- Message-level and rights management, using Advanced Encryption Standard (AES)-256 encryption
- Fine-grained message revocation, audit and control
- Capability to send hundreds of megabytes of data in a single e-mail
- Easy drag-and-drop experience
- Customizable interactions
- Machine learning and data analytics
- Appropriate levels of authentication
- Ease-of-use and simplicity
- Endpoint deployment options as a COM add-in or web add-in

### Principal Service Commitments and System Requirements

KnowBe4's management designs its processes and procedures related to the KSAT / PhishER / SecurityCoach system to meet its objectives. Those objectives are based on the service commitments that KnowBe4's management makes to user entities, the laws and regulations that govern the provisioning of the system, and the financial, operational, and compliance requirements that KnowBe4 has established for the services.

Commitments to user entities are documented and communicated in Service Level Agreements (SLAs), licensing agreements, Master Service Agreements (MSAs), and other customer agreements, as well as in the description of the service offerings online. Commitments and system requirements are standardized and include, but are not limited to, the following:

Trust Services Category	Service Commitments	System Requirements
Security	System access is granted to authorized personnel only Identification and remediation of security incidents/events	<ul style="list-style-type: none"> <li>• Logical access standards</li> <li>• Physical access standards</li> <li>• Encryption standards</li> </ul>
Availability	Production system uptime of 99.99% Ability to recover and restore customer data	<ul style="list-style-type: none"> <li>• System monitoring</li> <li>• Backup and recovery standards</li> </ul>
Processing Integrity	Customer reports will be complete Customer reports will be accurate	<ul style="list-style-type: none"> <li>• Data input validation standards</li> <li>• Report generation standards</li> </ul>
Confidentiality	Customer data will be maintained and protected from disclosure to unauthorized persons or entities	<ul style="list-style-type: none"> <li>• Data handling and retention standards</li> <li>• Data disposal standards</li> <li>• Multi-Factor Authentication standards</li> </ul>

Trust Services Category	Service Commitments	System Requirements
Privacy	Changes to privacy commitments will be communicated to customers	<ul style="list-style-type: none"> <li>Monitoring of applicable laws and regulations</li> <li>Personal information accessibility standards</li> <li>Data handling and retention standards</li> </ul>

## Components of the System

### Infrastructure

Primary infrastructure used to provide KnowBe4's Cloud Hosted Data Platforms System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Web Services	AWS Azure	Providing Cloud Hosting or part of the service delivery and infrastructure
Database Services	DynamoDB	RDS Database
Database Services	Aurora	Structured Query Language (SQL) Database
Database Services	MongoDB	NoSQL Database
Simple Storage Service Azure	S3 buckets Azure Blob Container	Object storage service

### Software

Primary software used to provide KnowBe4's Cloud Hosted Data Platforms System includes the following:

Primary Software		
Software	Operating System	Purpose
Datadog	Cloud based	Application log monitoring, system logging, application performance and error monitoring, and analytics
Salesforce	Cloud based	CRM
Zendesk	Cloud based	Ticketing system
Mixpanel	Cloud based	Business analytics
Pendo	Cloud based	Analytics
LaunchDarkly	Cloud based	Deploying new features through 'feature-flagging'
Active Directory (AD)	N/A	Identity and access management system

## People

KnowBe4 has seven main sectors: (1) Executive; (2) Revenue; (3) People Operations; (4) Finance; (5) Research & Development; (6) Product; (7) Courseware development.

The roles and responsibilities of key functions include the following:

- Chief Executive Officer (CEO): The CEO oversees the Executive Team and is responsible for the strategic vision and execution of the organization.
- Chief Product Officer (CPO): The CPO is the Head of Support and Product Management. The CPO is responsible for the tech direction of products and customer-facing issues.
- Chief Information Security Officer / Data Privacy Officer (CISO / DPO): The CISO / DPO is responsible for security and risk-related issues for the company and for the product. The CISO / DPO is also responsible for privacy-related issues.
- Chief Information Officer (CIO): The CIO is responsible for Internal IT including IT helpdesk, business process analytics, and business applications.
- Chief Financial Officer (CFO): The CFO is head of finance, accounting, and order processing.
- Chief Legal Officer: Responsible for contracts, privacy, agreements, and internal and external matters regarding litigation.
- EVP of Engineering: Responsible for leading and mentoring the Software Development, Quality Assurance, and Site Reliability Engineering teams.
- Chief Human Resources Officer (CHRO): Responsible for directing the people functions of the organization in accordance with the policies and practices of KnowBe4.
- Chief Learning Officer: Responsible for courseware design, content, creation, and delivery.

## Data

KnowBe4's Platform instances and data are hosted in various geographic AWS and Azure locations to comply with legal requirements and to provide better speed and reliability for customers. Here are the details of the locations where KSAT is running:

[https://support.knowbe4.com/hc/en-us/articles/45880984844179-KnowBe4-Data-Storage-Locations:](https://support.knowbe4.com/hc/en-us/articles/45880984844179-KnowBe4-Data-Storage-Locations)

- United States: AWS US-East-1 (Northern Virginia)
- Backup location: AWS US-West-2 (Oregon)
- Canada: AWS Central (Canada)
- Backup location: AWS EU-West-1 (Dublin, Ireland)
- European Union: AWS EU-West-1 (Ireland)
- Backup location: AWS EU-Central-1 (Frankfurt, Germany)
- United Kingdom: AWS EU-West-2 (London)
- Backup location: AWS EU-West-1 (Dublin, Ireland)
- Germany: AWS EU-Central-1 (Germany)
- Backup location: AWS EU-West-1 (Dublin, Ireland)

Data is managed and processed according to KnowBe4's corporate-level and Egress' product-specific data protection policies and procedures. Documents are marked according to their sensitivity and usage, and access to data and systems is only granted based on a business need-to-know. Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts.

Customer data is not utilized for testing in non-production environments. Confidential data, including production data and backup data, is encrypted at rest using AES-256 encryption, and access to manage encryption keys is restricted to authorized personnel. The transmission of confidential data is secured via an Internet connection encrypted with transport layer security (TLS) protocol, including e-mail exchanges with suppliers and customers. Documented data classification and retention policies are in place to help ensure that confidential data is properly maintained, restricted to authorized personnel, and prohibited from being used or stored outside of company-approved methods.

Documented data disposal procedures are in place to guide personnel on the procedures for the secure disposal of confidential data. Procedures are in place to dispose of customer data upon customer request and upon customer termination in accordance with the disposal commitments. The results of the data disposal are documented and tracked through resolution within the automated ticketing system.

Policies and procedures are documented to guide personnel in protecting and handling data and assets. Policies include, but are not limited to, the following:

- Data Handling and Protection Standards
- Data Retention and Destruction Policy

*Privacy Commitments*

The following table describes the information included as part of the Cloud Hosted Data Platforms System of KnowBe4:

Client Data	Reporting
<p>Types of client data collected</p> <ul style="list-style-type: none"> <li>• Business Contact information: employee first name, employee last name, manager first name, manager last name, organization, employee title, department, phone number, and business e-mail addresses</li> <li>• Automatically collected information: information collected via cookies and web beacons, including Internet protocol (IP) address, browser name, operating system details, domain name, date of visit, time of visit, pages viewed, or other similar information</li> <li>• Console Information: simulated phishing, security awareness testing and training results, risk score, security assessment results, training, and coaching information; and information uploaded to the Services</li> </ul>	<p>Reports provided:</p> <ul style="list-style-type: none"> <li>• Generated Information: phishing campaign results and metrics; security awareness training results; risk score; training and coaching information</li> </ul>

Defend:

Types of personal data collected:

- E-mail metadata received that could result in revealing personal data by inference:
- Sender address
- Subject
- Attachment names
- Sender Internet protocol (IP) Address (geolocation where possible)
- Other recipients on an e-mail
- Date/time of e-mail sent

Prevent:

Types of personal data collected:

- Portions and metadata of e-mails determined by the sender Hashed portions of e-mail body
- Hashed portions of e-mail attachments
- Attachment names

- Decisions of whether an e-mail is sent or advice is ignored

### Protect:

During account registration, the following data is requested from users:

- E-mail address
- First and Last name
- Password
- Security questions and answers, to assist in automatic password reset should the password be forgotten. Not required with OpenID
- (optional) Mobile telephone number, collected for the same purposes
- OpenID can be set up for free e-mail users of Google and Microsoft

In addition to this data, when registered users communicate to Protect servers, the product records IP addresses from the received requests. This includes key management requests.

Recipients, depending on configuration, may have the ability to download messages from Web Access in unencrypted form.

### Collection and Obtaining of Personal Information

KnowBe4 collects various types of personal information from individuals, user entities, or other third-parties to provide and improve its services. The types of personal information that may be collected include, but are not limited to:

- Contact details such as names, e-mail addresses, and phone numbers
- Employment-related information for workforce training and management
- User credentials and authentication data for system access
- IP addresses and device identifiers for IT security and system analytics

Information is gathered through direct user input during service registration, product use, support interactions, and through automated means such as tracking technologies when individuals interact with KnowBe4's services or website.

When user entities collect personal information, they may share relevant data with KnowBe4 as part of service provisioning or support. This transfer of information from user entities to KnowBe4 typically occurs through secure channels and application programming interfaces (APIs), or direct data uploads to KnowBe4's platforms, ensuring encryption and protection during the data transfer process.

### Requirements Identification

The process for identifying specific requirements in agreement with user entities, laws, and regulations applicable to the personal information is described in the following steps:

- a. **Agreements Review:** Legal and compliance teams conduct thorough reviews of contracts and data processing addendums with user entities. These documents often specify the types of personal information to be processed, data retention periods, and security measures to be maintained.
- b. **Legislation and Regulation Analysis:** Compliance officers scrutinize relevant privacy and data protection laws and regulations, which vary by location, industry, and the nature of the data processed.
- c. **Risk Assessment:** Annual risk assessments help identify specific areas where personal information is involved, and where contractual or legal obligations may apply.
- d. **Stakeholder Engagement:** Cross-functional meetings with stakeholders, such as the IT department, customer service, and human resources (HR), help gather insights into how personal information is processed across the organization. This collaborative approach ensures comprehensive identification of relevant requirements.

## Implementation of Controls and Practices

Once specific requirements are identified, the following steps are taken to implement controls and practices to meet these requirements:

- a. **Policy Development and Updating:** Based on identified requirements, policies governing the collection, storage, use, and disclosure of personal information are developed or updated. These policies form the framework of internal guidelines and practices regarding data handling.
- b. **Control Implementation:** Controls are instituted across the information lifecycle to ensure adherence to the requirements.
- c. **Training and Awareness Programs:** Employees are educated through training programs about their roles and responsibilities for protecting data. Regular updates and refreshers help reinforce best practices.
- d. **Monitoring and Auditing:** Continuous monitoring mechanisms, such as automated tools and periodic assessments, are deployed to ensure controls are effective and in place.
- e. **Incident Response Planning:** An incident response plan is established to manage and respond to data breaches or non-compliance issues promptly and in alignment with legal obligations. This plan includes clear procedures for internal escalation, external communication, and remediation.
- f. **Effective Communication:** Communication channels with user entities are maintained to report on compliance measures, data breaches, or any relevant changes in data protection practices that may impact the services provided.
- g. **Records of Processing Activities:** Records are kept detailing data processing activities, demonstrating alignment with identified requirements and providing audit trails.

Implementing these controls and practices requires a dynamic approach due to the evolving nature of data protection laws and technology. KnowBe4 remains vigilant and adaptable to maintain compliance and protect the personal information under their stewardship effectively.

## Data Protection

KnowBe4's Data Protection Highlights provide a concise overview of its policies for processing Personal Data, which include information that can personally identify individuals, such as names, e-mail addresses, and IP addresses. The organization collects Personal Data through various interactions with its services, including website visits, form submissions, and data uploads, as well as through data received from affiliates and third-party providers.

KnowBe4 uses this collected data to respond to inquiries, deliver services, manage its technology platforms, improve service offerings, address employment needs, and fulfill legal obligations.

For individuals who are not customers or end users but whose data KnowBe4 possesses, the organization provides a means to access, amend, or object to the processing of their Personal Data through an e-mail request. Those who are customers or end users, where services are provided under contract with their organization, the customer organization is responsible for their data, and individuals are advised to contact their organization's Account Owner or reach out to KnowBe4 for assistance in exercising their rights.

Personal Data may be shared with third-party partners for service provisioning and processing. These partners are contractually obligated not to use the data beyond the designated services. Knowbe4 does not sell Personal Data and allows for rights associated with data, including correction, objecting to processing, and consent withdrawal.

International data transfers are managed with protective measures compliant with regulatory standards.

The organization does not require or request sensitive information like protected health information (PHI), financial information covered by the Gramm-Leach-Bliley Act (GLBA), or payment card information protected by the Payment Card Industry Security Standard (PCI DSS) for its services. Where a customer provides this information, KnowBe4 offers additional contractual protections, where possible, to ensure that adequate protection is provided to such sensitive data.

### *Processes, Policies and Procedures*

Information security policies have been established to set the overall framework for managing the security of the IT infrastructure and applications. These policies are approved at the executive management level and establish standards for information security throughout KnowBe4's information resources. The Engineering Development team has primary responsibility for interpreting these standards, developing procedures and processes for implementing the standards, and overseeing logical security for KnowBe4 IT and applications. In addition, the Engineering Development team develops configuration standards for each type of hardware and associated system software. User administration processes for IT systems and applications are tied to the new hire and termination processes established by KnowBe4. Role-based access controls for least privilege with additional control requirements for single sign-on (SSO), Multi Factor Authentication (MFA), IP restrictions, and Virtual Private Network (VPN) have been defined.

### Physical Security

The in-scope system and supporting infrastructure are hosted by AWS and Azure. As such, AWS and Azure are responsible for the physical security controls for the in-scope system. Please see the "Subservice Organizations" section below for a detailed listing of controls owned by AWS.

Physical Security is out of scope for this assessment. KnowBe4 does not process or store any production or non-production data or systems locally. Physical security processes are considered in the shared responsibility model employed by AWS and Azure. KnowBe4 does have a physical security group responsible for securing the local facilities to protect the locations and people working onsite.

### Logical Access

Employees who no longer require access to the production environment are deactivated upon notification. A formal termination process has been implemented to ensure timely removal of access to systems. Quarterly access reviews are also performed to ensure access to systems within the environment is appropriate. Personnel with inappropriate access permissions are promptly disabled.

Access to the production system is controlled via SSO. Production system users are assigned role-based permissions. Administrator access to AWS and Azure is restricted to authorized personnel commensurate with their job roles and responsibilities and reviewed on a quarterly basis. Users are required to authenticate via multi-factor authentication.

KnowBe4's production systems are virtualized and hosted by AWS and Azure. AWS combined with multiple mechanisms within each allow flexibility to how access to data is controlled as well as how, when, and where it can be accessed. Amazon provides four different access control mechanisms: Identity and Access Management (IAM) policies, ACLs, bucket policies, and query string authentication. IAM enables organizations with multiple employees to create and manage multiple users under a single AWS account. With IAM policies, IAM users can be granted fine-grained control to Amazon S3 buckets or objects. ACLs can be used to selectively grant certain permissions on individual objects. Amazon S3 Bucket Policies can be used to grant or deny permissions across objects within a single bucket.

Amazon S3 supports the logging of requests made against Amazon S3 resources. Amazon S3 buckets are configured to create access log records for the requests made against it. The system access logs capture requests made against a bucket or the objects in it and can be used for auditing purposes.

KnowBe4 utilizes AWS security groups and applies them to systems to deny traffic and only allow specific services to the systems. Web Application Firewalls (WAFs) are also in place and configured to protect against external web-based attacks. WAF rules are applied at AWS CloudFront CDN as well as within the application itself (in-app WAF).

To access the production environment for the PDP products, users first authenticate to the cloud management consoles or the VPN via SSO and MFA. Once authenticated, users are then required to authenticate through the bastion host with a unique user ID and password. Once authenticated to the bastion host, users can then secure shell (SSH) or remote desktop protocol (RDP) to the production servers to which they have been granted access. Access to administer the production environment is restricted to authorized personnel and system administrators.

#### Computer Operations - Backups

KnowBe4 utilizes automated backup systems to perform scheduled backups of production data and systems on a regular basis, with configurations in place to alert administrators in the event of a failure. When an exception occurs, operational personnel perform troubleshooting to identify the root cause and ensure a successful backup is completed-either immediately or during the next scheduled cycle-in accordance with documented work instructions and customer preferences. To ensure the ongoing integrity and availability of data, KnowBe4 conducts restoration tests at least annually to verify that systems can be recovered from backups and to identify and prioritize response activities.

#### Computer Operations - Availability

KnowBe4 has established Business Continuity / Disaster Recovery (BCP/DR) plans that ensures the high availability of computer operations, which is pivotal to fulfilling the service commitments and objectives. Knowbe4 has a thorough framework, which encompasses redundancy, resilience, and disaster recovery protocols to address and mitigate potential service disruptions. Integral to the strategy is the proactive system monitoring and the robust business continuity plans, designed to withstand and rapidly recover from unforeseen incidents. Advanced tools are utilized for real-time system health monitoring, enabling prompt identification and remediation of issues potentially affecting availability. This effort is complemented by an environment designed to scale with a growing user base. The BCP/DR process is tested at least annually. In addition, the incident response protocol is a critical component of the availability strategy; it ensures timely and effective action to manage and mitigate the impacts of incidents, while adhering to strict service level requirements. Support teams stand ready to address and resolve issues, and deliver swift responses to uphold the high system availability. The incident response plan is also tested at least annually. Maintenance activities, incident management, and system statuses are made available to users via the company website.

#### Change Control

KnowBe4 has implemented a formal change management process that will allow staff to request, manage, approve, and control changes that modify services or systems within the KnowBe4 environments. The change control process is designed to enforce key development controls each time a change to the software is made, including development and emergency changes. The change management process begins with the identification, recording, and classification of the change, and continues with its review and approval, testing, and staging for implementation. Change requests are logged and tracked within a ticketing system. Once implementation has been completed, measured, and reported, the change process is complete.

The Engineering Development team has been structured to promote communication through each stage in the design process. This results in the Management team ultimately being responsible for ensuring development initiatives meet client needs and the strategic direction of the application including the transition from concept to production functionality. A code repository (change control software) tool is utilized and is combined with documentation of each release which provides for the ability to quickly revert to a previously functioning state version in the event that new code does not function as intended at any point in the development process. The ability to access and edit source code is restricted to personnel commensurate with their job role.

The code repository tool facilitates the development processes by systematically enforcing access controls, testing requirements, approvals, and deployments. Development work is done in a segregated environment. Failure of any tests, or failure to get approval as defined within the workflow, prevents the code from further progression within the code repository tool. Once the change has passed testing and the required approvals have been obtained, it is ready for deployment. A deployment automation tool is utilized to facilitate changes to the production environment. Product teams have authorization to deploy code only through the code repository tool which systematically enforces testing and approval rules prior to migration to production. Access to the production operating system and database systems is restricted to the infrastructure support teams.

### Data Communications

The internal network is protected from public Internet traffic via stateful inspection firewalls provided by AWS and Azure. The firewalls are configured to deny traffic and only allow specific services to a specific destination. Access to administer the firewalls is restricted to personnel commensurate with their job responsibilities. A security group controls the traffic allowed into a group of instances. For each security group, custom rules are added that govern the allowed inbound traffic to instances in the group. Other inbound traffic is denied. Rules for a security group can be modified dynamically and new rules are automatically enforced for existing and future instances in the group.

Encrypted communications are utilized to protect remote Internet sessions to the KnowBe4 applications and internal network. Encryption is used to ensure the privacy and integrity of the data being passed over the public network.

### **Boundaries of the System**

The scope of this report includes the Cloud Hosted Data Platforms System performed in the Clearwater, Florida facility.

This report does not include the cloud hosting services provided by AWS and Azure at multiple facilities.

### **Changes to the System Since the Last Review**

KnowBe4 has added three new product offerings to KnowBe4 Cloud Hosted Data Platforms, Protect, Defend, and Prevent. These products were acquired as of 2024 and have been brought into the scope of this report as of this reporting period.

### **Incidents Since the Last Review**

No significant incidents have occurred to the services provided to user entities since the organization's last review

### **Criteria Not Applicable to the System**

All Common/Security, Availability, Processing Integrity, Confidentiality, and Privacy criteria were applicable to the KnowBe4 Cloud Hosted Data Platforms System.

## Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Azure at multiple facilities.

### *Subservice Description of Services*

AWS and Azure provide cloud hosting services which include physical and environmental security controls over the cloud servers.

### *Complementary Subservice Organization Controls*

KnowBe4's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to KnowBe4's services to be solely achieved by KnowBe4 control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of KnowBe4.

The following subservice organization controls should be implemented by AWS and Azure to provide additional assurance that the trust services criteria within this report are met:

<b>Subservice Organization - AWS</b>		
<b>Category</b>	<b>Criteria</b>	<b>Control</b>
Common Criteria / Security	CC6.4 / CC7.2	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
Availability	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		All data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network rooms are connected to an Uninterruptible Power Supply (UPS) system and emergency generator power is available in the event of a loss of power. Google protects the information system from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.

**Subservice Organization - Azure**

Category	Criteria	Control
Common Criteria / Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

KnowBe4 management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, KnowBe4 performs monitoring of the subservice organization controls, including the following procedures:

- Holding discussions with vendors and the subservice organizations
- Reviewing attestation reports over services provided by vendors and the subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

#### **COMPLEMENTARY USER ENTITY CONTROLS**

KnowBe4's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to KnowBe4's services to be solely achieved by KnowBe4 control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of KnowBe4's.