Service Level Agreement Requirement Recommendations

Julie Embree

Department of Information Technology, SNHU

CYB-260: Legal and Human Factors of Cybersecurity

August 17, 2025

Service Level Agreement Requirement Recommendations

Control 6: Access Control Management

Access control management is a critical system control, as it defines protocols to "create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts". (CIS Controls, 2021).

The recommended CIS safeguards include the following (CIS Controls, 2021):

- Establishing access granting and revoking processes
    - Examples of granting access include newly hired employees or role changes for the user.
    - Examples of revoking access include an employee's termination or leaving the company, or role changes for the user. Account access should be disabled instead of deleted, to "preserve audit trails".
- Requiring multi-factor authentication (MFA) for externally exposed (or third-party) applications
    - MFA can be enforced "through a directory service or SSO [single sign-on] provider".
- Requiring MFA for remote network access or administrative access
- Establishing and maintaining inventories of authorization and authentication systems
    - Inventory reviews and updates should be carried out at least annually, to ensure that the system is up to date.
- Centralizing access control

    - Can be overseen “through a directory service or SSO provider”.
- Defining and maintaining role-based access control (RBAC)
    - Performed “through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties.” Reviews of the access controls should be carried out at least annually, to ensure that the authorized privileges are still appropriate.

Additionally, administrative or high-privileged accounts should not be used for all activities but only used for tasks which require administrator authorization. (CIS Controls, 2021).

These access control safeguards should be integrated into Fit-vantage’s security protocols. This will boost system security by enforcing the principle of least privilege, which grants users the minimum amount of system access necessary to perform their duties. (Gramma, 2022, p. 487). As this control is specified in the service level agreement (SNHU, *SLA*, 2025), it reflects Helios Health’s existing commitment to maintaining effective access control management.

Control 14: Security Awareness and Skills Training

Security awareness and skills training is another critical system control, as it influences “behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks”. (CIS Controls, 2021). Training must be provided for all employees – regardless of role or seniority – in order to be effective.

The recommended CIS safeguards include the following (CIS Controls, 2021):

- Establishing and maintaining a security awareness program

    - Training should be conducted for new hires upon arrival, and for all employees at least annually. The content should be reviewed and updated at least annually, or "when significant enterprise changes occur that could impact this Safeguard."
- Training all employees to recognize social engineering attacks
    - Attacks can include "phishing, pre-texting, and tailgating" amongst other types.
- Training all employees on authentication best practices
    - Examples of authentication include "MFA, password composition, and credential management".
- Training all employees on data handling best practices and causes of unintentional data exposure
    - Data handling best practices include "how to identify and properly store, transfer, archive, and destroy sensitive data", using screen locking, "erasing physical and virtual whiteboards", and "storing data and assets [devices] securely".
    - Data exposure training includes "mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences".
- Training all employees on recognizing and reporting security incidents
- Training all employees on identifying and reporting missing security updates
    - Includes verifying and reporting "out-of-date software patches", automated processes or tool failures, and "notifying IT personnel of any failures".

- Training all employees on insecure network dangers
    - Includes the “dangers of connecting to, and transmitting data over, insecure networks” and (for remote employees) guidance on how to “securely configure their home network infrastructure”.
- Conducting role-specific training

To strengthen its overall security posture, Fit-vantage should incorporate these security awareness and training controls into its protocols. This will boost system security by ensuring all employees are properly trained on cyber risks, how to avoid mishandling data, and how to respond by alerting appropriate personnel. This control is also outlined in the service level agreement (SNHU, *SLA*, 2025), indicating that Helios Health has already acknowledged the importance of robust security awareness and skills training.

Training Program Example: Phishing

Phishing poses a significant threat across a variety of industries and is anticipated to advance with more diverse and sophisticated attack methods. Targets are increasingly focused on “high-impact campaigns, particularly against HR, finance, and payroll”. (Fitzgerald, 2025). Additionally, threat actors have incorporated generative AI in their toolset and are able to “create more convincing, personalized phishing messages in minutes, automate large-scale polymorphic campaigns, and improve their odds of bypassing detection.” (Fitzgerald, 2025). The click rate for AI-made phishing emails is over “four times that of human-written emails”, making it a quick and profitable resource for threat actors. (Fitzgerald, 2025).

Phishing takes a variety of forms and targets, including the following (Kim and Solomon, 2023, p. 107-108, p. 520):

- Smishing
    - Attack by SMS (text) messages to the target's cell phone.
- Spear phishing or whaling
    - Attack by email or instant message that uses fraud against a specific organization (or an executive) to gain "unauthorized access to confidential data."
- Vishing
    - Attack by telephone that uses coercion tactics to gain personal information from the target.

Training Program's Expected Outcomes

As Fit-vantage will become a partner to Helios Health (a health insurance company), it will likely face an increased rate of phishing attacks because healthcare companies are a high target from threat actors. Because of the regularity and nature of phishing attacks, it is pivotal to incorporate examples, phishing tests, click rate assessments, and post-training evaluations (or employee feedback) into Fit-vantage's training program. System weaknesses can be found by monitoring phishing incidents and analyzing the metrics of the attacks. (I & T Today, n.d.).

A recent comparative study found that, one year after implementing comprehensive security awareness training, healthcare organizations improved their phish-prone percentage (PPP) or phishing vulnerability by an 88.8% reduction. (Collard et al., 2024). Furthermore, by embedding phishing awareness into its broader security strategy, Fit-vantage can mitigate the financial risk of cyberattacks—an expense that averages $1.6 million for small and mid-sized businesses. (Gundersen, 2022).

References

CIS Controls. (May 2021). *CIS Critical Security Controls® Version 8*. Center for Internet Security. https://learn.snhu.edu/content/enforced/1969530-CYB-260-10771.202556-1/course_documents/CYB%20260%20CIS%20Controls%20Version%208.pdf?isCourseFile=true&ou=1969530

Collard, Anna et al. (2024). *Phishing by Industry Benchmarking Report 2024 Edition*. KnowBe4. https://formits.com/wp-content/uploads/2024/06/2024-Phishing-by-Industry-Benchmarking-Report-EN_US.pdf

Fitzgerald, Anna. (August 14, 2025). *60+ Phishing Attack Statistics: The Facts You Need To Know for 2026*. Secureframe. https://secureframe.com/blog/phishing-attack-statistics

Gramma, Joanna Lyn. (2022). *Legal and Privacy Issues in Information Security, 3rd Edition*. Jones & Bartlett Learning.

Gundersen, Gry Myrtveit. (January 5, 2022). Does Phishing Training Work? Yes! Here's Proof. CyberPilot. https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof

I & T Today. (n.d.). *Measuring Effectiveness of Phishing Email Training for Employees. Innovation & Tech Today*. https://innotechtoday.com/measuring-effectiveness-of-phishing-email-training-for-employees/

Kim, David and Solomon, Michael G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones & Bartlett Learning.

SNHU. (2025). *Service Level Agreement*. Southern New Hampshire University, CYB 260. https://learn.snhu.edu/content/enforced/1969530-CYB-260-10771.202556-1/course_documents/CYB%20260%20Service%20Level%20Agreement.pdf?isCourseFile=true&ou=1969530

SNHU. (2025). *Project Three Scenario*. Southern New Hampshire University, CYB 260. https://learn.snhu.edu/content/enforced/1969530-CYB-260-10771.202556-1/course_documents/CYB%20260%20Project%20Three%20Scenario.pdf?isCourseFile=true&ou=1969530