

Arctic Wolf Managed Security Awareness®

COMPLIANCE CONTENT PACK



There are many different regulations for which organizations and businesses need to train their employees. Often, these topics are unique, and a “one-off training” is delivered by different platforms. This can be a challenge for administrators to manage and employees to navigate.

That’s why having a professional and streamlined training experience for your employees helps improve participation while reducing administration bandwidth and cost. And it’s why we created the Compliance Content Pack.

This collection of compliance training courses is available as an add-on for all Managed Security Awareness customers. The Compliance Content Pack currently offers 16 compliance training courses for PCI, HIPAA, FERPA, and other important regulations. All courses are delivered through the Arctic Wolf® Aurora Platform, and delivered together with your security awareness program.

Developed in-house and used by organizations across industries, Arctic Wolf now makes it simple to add compliance training to your security awareness program. The compliance lessons can be assigned to any Microsoft Entra ID (formerly Azure AD) group and tracked from within the same dashboard by customer administrators. You have the flexibility to use any of the compliance courses you’d like by assigning them to different groups within your organization.

Compliance training requires a different approach than our security awareness microlearning content. Compliance lessons are optimized for new employees and designed to meet yearly compliance obligations of current employees as required by industry and government regulations.

The compliance content includes everything required for each compliance topic and can usually be completed within 25 to 30 minutes.

Compliance Training Topics

Finance Focus

- PCI for Users, IT, and Managers

Healthcare Focus

- HIPAA Compliance Courses (Essentials, Privacy Rule, and Security Rule)
- OSHA: Airborne and Bloodborne Pathogens

Higher Education Focus

- Title IX
- FERPA

HR Focus

- Anti-Discrimination
- Sexual Harassment Prevention (General and CA State-Specific)
- Affirmative Action and Equal Employment
- Family Medical Leave Act (FMLA)

Security Focus

- Security Essentials
- General Data Protection Regulation (GDPR)

CCP is an optional component of Arctic Wolf Managed Security Awareness. It is designed to minimize human risk with 100% relevant content that employees will actually pay attention to.



A Well-Rounded Security Awareness Program

Training employees for security threats should never involve a one-and-done approach, and meeting compliance standards doesn't necessarily mean your employees are ready to face the cyber threats of today.

However, pairing training courses that meet compliance standards in combination with an ongoing security awareness training with a phishing simulation component makes for a powerful and comprehensive program.



The Arctic Wolf Compliance Content Pack is not just another bundle of long videos. Your compliance training content is interactive with navigable chapters and quizzes. This maximizes the effectiveness of the training for your company.

Arctic Wolf Managed Security Awareness provides relevant and engaging ongoing training, while the Compliance Content Pack adds the ability to meet certain regulatory standards and train on the unique topics they require.



Note: Arctic Wolf's Compliance Content Pack requires customers to synchronize their users via Microsoft Entra ID (formerly Azure AD) with the Arctic Wolf® Aurora Platform. This allows the program administrators to assign compliance content to groups of users.



Finance

PCI Essentials

Designed for end users, this PCI course provides an overview of PCI protections and safeguards including the handling of suspected breaches with a focus on identification, reporting, and prevention measures.

Course Outline: 12-14 minutes + quiz

1. Introduction to the PCI Data Security Standards
2. Types of Data Protected by PCI Compliance
3. The Importance of PCI Compliance
4. Physical Security Safeguards for Protecting Cardholder Data
5. Technology Safeguards for Protecting Cardholder Data
6. Securing CNP Transactions
7. What to Do When You Suspect a Breach

PCI for IT and Management

This course provides a high-level overview of each of the PCI requirements and control objectives. It also discusses the physical security of cardholder data, including the handling of receipts, system passwords, and point-of-sale systems. This course will help both technical and non-technical employees adhere to the PCI data protection standards.

Course Outline: 12-14 minutes + quiz

1. Introduction to the PCI Data Security Standards
2. The PCI Control Objectives and Requirements
3. Understanding PCI's 12 Requirements
4. Physical Security Safeguards



Healthcare

HIPAA Essentials

This course offers a comprehensive introduction to HIPAA. It addresses the use, disclosure, and protection of patients' health care information, as well as the steps to take when a breach of protected health information (PHI) occurs.

Course Outline: 25–30 minutes + quiz

1. Introduction to HIPAA
2. Identifying Protected Health Information (PHI)
3. Verifying Identity When Information Is Requested
4. Minimum Necessary Standard for Disclosure of PHI
5. Patient Rights Regarding Their PHI
6. Notice of Privacy Practices
7. The Security Rule and Protecting PHI
8. HIPAA Enforcement
9. When a Breach Has Occurred
10. Penalties for Violating HIPAA

HIPAA Privacy Rule

This course addresses the use and disclosure of an individual's health information and equips employees with the knowledge to uphold the HIPAA Privacy Rule required standards.

Course Outline: 14–16 minutes + quiz

1. Introduction to HIPAA
2. Important Definitions Associated With the HIPAA Privacy Rule
3. Information Covered by the Privacy Rule
4. How to Handle Requests for PHI
5. Appropriate Use and Disclosure Under the Privacy Rule
6. Patient Rights Under the Privacy Rule
7. Privacy Practices and Breaches of Confidentiality
8. Notices of Enforcement Discretions Due to COVID-19



Healthcare

HIPAA Security Rule

This course offers specific training on the national protections given to health information that is held or transferred in electronic form.

Course Outline: 10-12 minutes + quiz

1. Introduction to the HIPAA Security Rule
2. The Need for the Security Rule
3. Covered Entities and the Security Rule
4. Responsibilities for Organizations
5. Responsibilities for Employees

OSHA: Airborne and Bloodborne Pathogens

This course covers standard precautions for preventing the transmission of infectious diseases in accordance with OSHA's standards regarding Airborne and Bloodborne Pathogens.

Course Outline: 14-16 minutes + quiz

1. Defining Standard Precautions
2. Bloodborne Pathogens and How They Are Transmitted
3. Diseases Transmitted by Bloodborne Pathogens
 - a. Hepatitis B
 - b. Hepatitis C
 - c. Human Immunodeficiency Virus
4. Airborne Pathogens and How They Are Transmitted
5. Diseases Transmitted by Airborne Pathogens
 - a. Tuberculosis
 - b. Measles
 - c. Varicella
6. Standard Precautions for Preventing Transmission



Higher Education

FERPA

This course provides training on the requirements for handling student information, including educational records, directory information, parental rights, and more.

Course Outline: 12-14 minutes + quiz

1. Introduction to FERPA
2. Education Records
3. Exceptions to Written Permission
4. Rights of Students Under FERPA
5. Rights of Parents Under FERPA
6. Disclosing and Withholding Information

Title IX

A comprehensive introduction to the accommodations and protections provided by Title IX. A series of scenarios allow employees to place themselves in different situations that may take place on and around campus.

Course Outline: 30-35 minutes + quiz

1. Introduction to Title IX
2. Who Is Protected Under Title IX?
3. Defining Sexual Harassment
4. Types of Sexual Harassment
5. Other Important Gender-Based Misconduct Policies and Laws
6. Bystander Intervention Strategies
7. Reporting Sexual Misconduct
8. Protection Against Retaliation
9. Supporting a Student Who Has Been Sexually Assaulted



Human Resources

Affirmative Action and Equal Employment

Arctic Wolf's Affirmative Action and Equal Employment course provides an overview of Affirmative Action and Equal Employment laws and the important role they play in removing inequality from the workplace.

Course Outline: 10-12 minutes + quiz

1. Introduction to Equal Opportunity Employment
2. Equal Opportunity Employment Classes
3. Introduction to Affirmative Action
4. Covered Employers
5. Underutilized Groups
6. Important Questions to Consider
7. Affirmative Action Controversies and Misconceptions
8. Additional Laws to Consider

Anti-Discrimination

Discrimination does not belong in the modern workplace. Arctic Wolf's Anti-Discrimination Awareness and Compliance course will help your employees understand what discrimination is, what the law says about discriminating against employees and potential employees, and learn what to do to prevent and respond to discrimination in the workplace.

Course Outline: 10-12 minutes

1. Defining Discrimination
2. What the Law Says About Discrimination
3. Effects of Discrimination
4. Reducing and Preventing Discrimination



Human Resources

Sexual Harassment Awareness (General, Non-State Specific)

This Sexual Harassment Awareness course provides an understanding of federal law and employer responsibilities. The course helps define a hostile work environment, and outlines how to report sexual harassment incidents.

Course Outline: 10–12 minutes + quiz

1. Defining Sexual Harassment
2. Categories of Sexual Harassment
3. Types of Sexual Harassment
4. Identifying When Sexual Harassment Occurs
5. Preventing Sexual Harassment in the Workplace
6. What Title VII Says About Sexual Harassment

Sexual Harassment Prevention for Employees (State of CA)

This course helps non-supervisory employees understand their role in creating and maintaining a harassment-free environment. This course meets California state law requirements for employees to receive one hour of sexual harassment prevention training.

Course Outline: Divided into 2 modules: total 1 hour

1. Sexual Harassment Laws – Federal and California Law
2. Defining Sexual Harassment
3. Who Is Protected?
4. Types and Forms of Sexual Harassment
5. Reasonable Approach
6. Liability
7. Workplace Rights and Remedies
8. Policies and Procedures
9. Best Practices



Human Resources

Sexual Harassment Prevention for Supervisors (State of CA)

This course trains supervisors to understand their role in creating and maintaining a harassment-free environment. This course meets California state law requirements for supervisors (including managers and executives) to receive two hours of sexual harassment prevention training.

Course Outline: Divided into 3 modules: total 2 hours

1. Sexual Harassment Laws – Federal and California Law
2. Defining Sexual Harassment
3. Who Is Protected?
4. Types and Forms of Sexual Harassment
5. Reasonable Approach
6. Liability
7. Workplace Rights and Remedies
8. Policies and Procedures
9. 5-Point Tool for Evaluating Behavior
10. Best Practices
11. Supervisor's Role in Creating a Sexual Harassment-Free Work Environment

The Family and Medical Leave Act (FMLA)

This course provides an overview of federal requirements for FMLA.

Course Outline: 10-12 minutes + quiz

1. Introduction to FMLA
2. Requirements for Employers
3. Employee Eligibility Criteria
4. Types of Leave
5. Leave Requirements
6. Administrative and Notice Requirements
7. Employment and Benefit Protection
8. Enforcement of FMLA



Security

Security Essentials

This course details the main ways in which an employee can practice good cyber hygiene in the workplace.

Course Outline: 20–25 minutes + quiz

1. Data Breaches and Their Impact
2. Secure Computer Use
3. Secure Internet Use
4. Secure Email Use
5. Viruses, Spyware, and Malicious Code
6. Password Selection and Management
7. Social Engineering Tactics
8. Defending Against Social Engineering
9. Secure Wireless Networking
10. Secure Travel and Remote Work
11. Reporting Incidents

NEW

General Data Protection Regulation (GDPR)

Designed for end users, this course provides an overview of GDPR principles and protections of personal data with a focus on GDPR compliance.

Course Outline: 20 minutes + quiz

1. Introduction to the General Data Protection Regulation (GDPR)
2. What is GDPR, and who must comply
3. The key terms and concepts of GDPR
4. The GDPR's principles
5. How the GDPR affects European Union member states
6. How the GDPR affects countries outside of the European Union
7. The rights of data subjects
8. Staying GDPR compliant
9. An organization's roles and responsibilities

This information is not legal advice and should not be interpreted as such. Consult with your own legal counsel to determine your regulatory obligations and assess the effectiveness of your compliance programs. Arctic Wolf products and services are not compliance solutions but are tools that can support your compliance programs.



©2025 Arctic Wolf Networks, Inc., All Rights Reserved. Arctic Wolf, Arctic Wolf Platform, Arctic Wolf Security Operations Cloud, Arctic Wolf Managed Detection and Response, Arctic Wolf Managed Risk, Arctic Wolf Managed Security Awareness, Arctic Wolf Incident Response, and Arctic Wolf Concierge Security Team are either trademarks or registered trademarks of Arctic Wolf Networks, Inc. or Arctic Wolf Networks Canada, Inc. and any subsidiaries in Canada, the United States, and/or other countries.

SOC2 Type II Certified



ISO 27001
CERTIFIED
CYBERGUARD
COMPLIANCE