

Microsoft 365 Data Security Engineering

ARC403

Stand up a working data security program in a Purview tenant. Classify what the business actually holds, label it so every downstream control can act, close the channels data leaves through, set retention that satisfies the regulator, watch the people who already have access, and investigate when something moves.

Modules	21
Lessons	185
Phases	7
Free preview	Course Orientation (7 lessons)

The method

Data security in Microsoft 365 is a chain, and every link is inert without the one before it. This course runs it in the order it has to work.

1. Classify before you protect. Every Purview control resolves to a classification. Labels, DLP and retention all ask the same question first, and an estate that never answered it cannot enforce anything.
2. Label so the protection travels. A sensitivity label carries its protection out of the tenant with the file. That is the difference between a control and a boundary.
3. Automate the labeling, because users will not. Manual classification at scale is a policy nobody follows. Auto-labeling is what makes coverage real.
4. Write DLP against what actually leaves. Policy tuned against a hypothesis blocks legitimate work and misses the path in use. Run in simulation and read the result first.
5. Investigate what the controls reported. Alerts, insider risk signals and the audit record, read as an investigation rather than a queue.

The course closes with configuration guides for every control it built.

What this course assumes

No minimum experience and no prerequisite course. The Purview surface, the classification model and the licensing that gates each control are introduced where they first matter.

What makes it go faster: a tenant with the relevant Purview licensing, since much of this is gated. Not required, and the course is explicit about which control needs which tier.

What this course does not cover: incident response process, identity security and endpoint engineering, which are separate courses. This is protecting the data itself.

Full syllabus

Course Orientation

Course Orientation FREE PREVIEW

What this course teaches: how to build data security in a Purview tenant that has the license and none of the configuration.

1. 0.1 What Data Security Engineering Is
2. 0.2 The Purview Surface
3. 0.3 How This Course Is Structured
4. 0.4 Where This Shows Up
5. 0.5 What Purview Cannot Do
6. 0.6 Following Along
7. Module Summary

Phase 1: Know your data

The Data Security Problem

Why data security is a different job: data has three states and a control that works in one does nothing in the others.

1. 1.1 The Three States of Data
2. 1.2 A Document Is a Population
3. 1.3 Purview as a Control Plane
4. 1.4 The Classification Engine
5. 1.5 Licensing: Capabilities, Not Features
6. 1.6 The Boundary
7. 1.7 The Compliance Role Groups
8. 1.8 Least Privilege When the Privilege Is Reading Everything
9. 1.9 The Global Admin Anti-Pattern
10. 1.10 What a Program Actually Is
11. Module Summary
12. Check My Knowledge

Classification

Classification is the datum every other Purview control resolves to.

1. 2.1 Sensitive Information Types and the Confidence Model
2. 2.2 Building a Custom SIT and Proving It Works
3. 2.3 Document Fingerprinting
4. 2.4 Exact Data Match: The Schema
5. 2.5 Exact Data Match: Hashing, Upload, and Refresh
6. 2.6 Trainable Classifiers
7. 2.7 OCR and What It Cannot Read
8. 2.8 Data Explorer and Content Explorer
9. 2.9 Measuring and Tuning Classification
10. 2.10 The Classification Decision
11. Module Summary
12. Check My Knowledge

Phase 2: Mark your data

Sensitivity Labels

The label is the only control that leaves your tenant.

1. 3.1 The Label That Travels
2. 3.2 The Fourteen-Label Failure
3. 3.3 Designing a Taxonomy
4. 3.4 Label Scope
5. 3.5 Content Marking
6. 3.6 Encryption: What It Actually Does
7. 3.7 The Encryption Trade
8. 3.8 Publishing
9. 3.9 Priority and Precedence
10. 3.10 The Taxonomy Decision
11. Module Summary
12. Check My Knowledge

Auto-labeling and Containers

Client-side against service-side and why the difference is operational.

1. 4.1 The Method Field Changes
2. 4.2 Client-Side and Service-Side
3. 4.3 Simulation Is Not Optional
4. 4.4 Reading a Simulation
5. 4.5 The Policy That Never Finishes
6. 4.6 Container Labels
7. 4.7 The Container-Item Distinction
8. 4.8 Default Labels on a Library
9. 4.9 Defender for Cloud Apps
10. 4.10 What Automation Costs
11. Module Summary
12. Check My Knowledge

Beyond the Tenant

Where the label stops traveling. The Purview Information Protection client and the scanner against on-premises file shares. Message Encryption and Advanced Message Encryption for mail that leaves your control.

1. 5.1 Where the Label Stops Traveling
2. 5.2 The Information Protection Client, and What It Is Not
3. 5.3 The File Labeler and PowerShell on Files Office Never Opens
4. 5.4 The Scanner: What It Is and What It Needs
5. 5.5 Discovery Before Enforce
6. 5.6 Reading a Scan, and What It Silently Skips
7. 5.7 Encryption Blinds the Scanner
8. 5.8 Message Encryption: Protecting Mail That Leaves
9. 5.9 Advanced Message Encryption: Expiration and Revocation
10. 5.10 The Estate You Can and Cannot Reach
11. Module Summary
12. Check My Knowledge

Phase 3: Stop it leaving

DLP Policy Design

Design a DLP policy from a requirement, not a template.

1. 6.1 Requirements to Policy
2. 6.2 Locations
3. 6.3 Conditions
4. 6.4 Actions
5. 6.5 Overrides and Notifications
6. 6.6 Roles and Permissions
7. 6.7 Rule Precedence
8. 6.8 Policy Precedence
9. 6.9 Simulation to Block
10. 6.10 File Policies in Cloud Apps
11. Module Summary
12. Check My Knowledge

Endpoint DLP

Endpoint DLP as a discipline. The device as a different surface, onboarding as the gate, browser and file-type reality, the six egress channels, advanced device rules, the exclusion model, and just-in-time protection.

1. 7.1 Endpoint DLP Is a Different Discipline
2. 7.2 Onboarding Is the Gate
3. 7.3 The Browser and File-Extension Reality
4. 7.4 What the Agent Sees, and How You Watch It
5. 7.5 Channels I: Removable Media and Network Shares
6. 7.6 Channels II: Cloud Upload and Restricted Apps
7. 7.7 Channels III: Print and Clipboard
8. 7.8 Advanced Device Rules
9. 7.9 The Exclusion Model
10. 7.10 Just-in-Time Protection
11. Module Summary
12. Check My Knowledge

Phase 4: Keep and dispose

Retention and Records

Retention as a two-sided obligation: keep content as long as it must be kept, and dispose of it deliberately when the obligation ends.

1. 8.1 Retention Is Two Obligations
2. 8.2 Labels vs Policies
3. 8.3 What Retention Does to an Item
4. 8.4 Static and Adaptive Scopes
5. 8.5 Publishing and Auto-Apply
6. 8.6 Precedence: The Four Principles
7. 8.7 A Worked Conflict and Policy Lookup
8. 8.8 Recovering Retained Content
9. 8.9 Disposition and Review
10. 8.10 The Records Management Boundary
11. Module Summary
12. Check My Knowledge

Phase 5: Watch and investigate

Insider Risk Management

Watching the people who handle your data, powerfully and lawfully.

1. 9.1 What Insider Risk Management Is
2. 9.2 Roles, Permissions, and Separation of Duties
3. 9.3 The Privacy Model
4. 9.4 Connectors and the HR Connector
5. 9.5 Signal Sources and the Endpoint
6. 9.6 Templates, Indicators, and Thresholds
7. 9.7 Forensic Evidence Settings
8. 9.8 Adaptive Protection
9. 9.9 Alerts, Cases, and Notices
10. 9.10 Standing Up Insider Risk Management for Northgate
11. Module Summary
12. Check My Knowledge

Investigation

The data-security engineer as investigator.

1. 10.1 The Engineer as Investigator
2. 10.2 Purview Audit: Standard and Premium
3. 10.3 Audit Retention and the Gap That Ends Investigations
4. 10.4 Searching the Unified Audit Log
5. 10.5 Activity Explorer: The Label and DLP Trail
6. 10.6 Responding to DLP Alerts
7. 10.7 Purview Alerts in Defender XDR
8. 10.8 Cloud App File and Activity Alerts
9. 10.9 Content Search: Collecting the Evidence
10. 10.10 Correlating Endpoint and Cloud
11. Module Summary
12. Check My Knowledge

Phase 6: AI and configuration guides

Data Security for AI

Securing data for AI in Microsoft Purview.

1. 11.1 Why AI Changes the Data Security Problem
2. 11.2 DSPM for AI: The Front Door
3. 11.3 Prerequisites and Onboarding
4. 11.4 Data Risk Assessments and Oversharing
5. 11.5 Sensitivity Labels as the Copilot Control
6. 11.6 DLP for Microsoft 365 Copilot
7. 11.7 Oversharing Controls in SharePoint
8. 11.8 Third-Party AI and the Endpoint
9. 11.9 Prompt and Response Governance
10. 11.10 The Copilot Readiness Baseline
11. Module Summary
12. Check My Knowledge

Configuration Guides

Step-by-step configuration guides for every control in the data-security program.

1. 12.1 Classification: Custom SITs and Exact Data Match
2. 12.2 Sensitivity Labels and Auto-labeling
3. 12.3 DLP and Endpoint DLP
4. 12.4 Retention and Records
5. 12.5 Insider Risk and Adaptive Protection
6. 12.6 Data Security for AI

Phase 0: Course Resources

Cheatsheets

Where each control lives, what its setting actually decides, and what it leaves uncovered, one sheet per domain.

1. Classification
2. Platform and Permissions
3. Sensitivity Labels
4. Auto-labeling and Containers
5. Beyond the Tenant
6. DLP Policy Design
7. Endpoint DLP
8. Retention and Records
9. Insider Risk Management
10. Investigation
11. Data Security for AI
12. Deployment Order
13. Building It: Create Commands

Cookbooks

Ordered procedures for the data security work that recurs: standing up classification, rolling out labels, deploying DLP without stopping the business.

1. Rolling Out Sensitivity Labels
2. Deploying DLP Without Stopping the Business
3. Getting Ready for Copilot
4. Building a Classifier That Works
5. Responding to a Data Incident
6. Designing Retention That Deletes
7. Standing Up Insider Risk

Lab Setup

Building a tenant with content messy enough to behave like a real estate, where you can watch a control cover nothing.

1. The Tenant and What It Carries
2. Planting Content That Misbehaves
3. Deploying Controls and Watching Them Miss
4. Breaking It on Purpose
5. Verify, Delays, and What the Lab Cannot Teach

Walkthroughs

Data security work reasoned end to end, including the cases where the control was already there and the ones that end in doing nothing.

1. The DLP Number That Meant Nothing
2. The Copilot Deadline
3. The Encryption Request That Should Be Refused
4. The Exfiltration That Was a Backup
5. The Policy That Protected Nothing
6. The Deletion That Never Happened

Playbooks

What to do when something fires or somebody asks: a DLP alert, a suspected leak, a subject access request, a regulator, a control that broke the business.

1. A DLP Alert Fires
2. Content Has Left and Somebody Knows
3. A Subject Access or Deletion Request
4. A Control Has Broken the Business
5. A Regulator or Auditor Asks
6. Somebody Is Leaving With Access
7. Somebody Found Content They Should Not See

Playground

Every practice surface available for this course, what each one gives you, and where the gaps are.

References & Further Reading

Microsoft Purview documentation, Microsoft security documentation, sensitive information type and EDM references, DLP and endpoint guidance, retention and records, insider risk, DSPM for AI, and the frameworks and standards used throughout the course.

1. DS100.1 References & Further Reading

Course Completion

Course Exam

Microsoft 365 Data Security Engineering end-of-course exam: a simulation-based assessment testing whether you can scope a data security incident, establish what a label and a policy actually did, and respond without breaking the business process that produced the data.

1. Course Completion. Microsoft 365 Data Security Engineering

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/m365-data-security/