RIMtech Online Training

RIMtech
www.rimtechconsulting.com

Advanced Purview Compliance Training

Microsoft Purview Information Protection

Defensible Deployment for IT, Compliance & Records Professionals

Duration
8 hours (1 day)

Microsoft Purview Information Protection is easy to learn. Deploying it correctly is where the real challenge lies. Most Purview training teaches features. It shows you where the buttons are, what the settings do, and how to navigate the interface. But organizations need to know how to deploy it to reduce risk, protect sensitive information, satisfy compliance obligations, and support the business without disrupting productivity.

This intensive one-day course is designed primarily for IT professionals responsible for implementing and supporting Microsoft Purview, and also for records management, privacy, legal, and compliance professionals who must ensure that Information Protection is deployed appropriately. Rather than providing another feature tour, this course teaches the critical decisions, governance principles, deployment strategies, and real-world implementation techniques required to achieve defensible protection. You will learn how to:

- Prevent accidental or nefarious data loss/leakage
- Identify sensitive information at scale
- Automatically apply appropriate protection to sensitive information
- Apply markings to sensitive information
- Manage external sharing of information

Instructor Bruce Miller draws upon decades of experience in electronic recordkeeping, information governance, compliance, and Microsoft technologies. You will learn how to configure Information Protection so that it aligns with your business requirements, regulatory obligations, privacy expectations, and operational realities. You will discover not just what Purview can do, but when, why, and how its capabilities should be deployed to maximize protection, minimize risk, and avoid creating unnecessary barriers for users.
In this course you'll discover how to protect sensitive information, prevent data leakage, enable secure collaboration, govern AI access to information, and more. Not just what Purview can do, but how to deploy it effectively for maximum compliance. You will understand how to deploy Microsoft Purview Information Protection with confidence — in a manner that is technically sound, operationally practical, and legally defensible.

RIMtech

CATALYST
Information Governance Tools

Learning Objectives

Upon completion of this workshop, participants will be able to:

- How to reduce accidental or nefarious leakage of sensitive information
- Avoid unintended data sharing via AI Searching
- Identify sensitive information across various data sources
- Apply appropriate sensitivity labels without user intervention
- Secure entire collaboration spaces
- Automatically apply markings to documents and messages to help enforce protection
- Control external sharing of sensitive information
- Allow users to override controls without compromising compliance

Who Will Benefit

IT Professionals responsible for eDiscovery deployment, Legal Counsel, Privacy Officers, Records and Information Professionals.

Takeaway Tools

Participants are supplied with all course materials, including diagrams and summaries of Purview capabilities.

Certification Credits

7 CEUs | 7 CEUs | 8 CEUs

Testimonials

"*I loved the performance measure aspect, and 20 suggested decisions. This was worth the cost of the course alone.*"

"*I really liked the presenter. He engaged the attendees and asked thought-provoking questions that generated some lively conversations.*"

"*This was one of the most engaging and informative seminars I can remember attending. I got a lot of great takeaways and can enthusiastically tell my employer that this was a productive use of my time and training dollars.*"

"*Thank you! This course hit the nail on the head – it touched on many of the issues that I see in the workplace and provided me with the guidance and affirmation that will help me to manage these issues. Awesome seminar!*"

Instructor

Bruce Miller, MBA, IGP is a world leading expert on electronic recordkeeping. He is an independent consultant, an author, and an educator. Widely regarded as the inventor of modern electronic recordkeeping software, he pioneered the world's first commercial electronic recordkeeping software in 1989. In 1997 he achieved the world's first e-Records software certification against the US DoD 5015.2-STD standard, and has since presided over several successful software certifications. In 1999 he developed the world's first e-Records software ***engine*** for business software. That year he received ARMA Canada's National Capital Region's **Ted Ferrier Award of Excellence** for his contribution to the field of records management. Bruce's software was the first technology in the world to be certified against the revised 5015.2 June 2002 standard. In 2002 his company was acquired by IBM, where he served for three years as IBM's global e-Records Strategy and Business Development Executive. At IBM he was honored as a *Technical Leader*, one of only 439 out of 360,000 IBM employees. Mr. Miller is the recipient of the prestigious **Emmett Leahy Award**, considered the highest international recognition given to professionals in the field of information and records management. His book "*Managing Records in Microsoft SharePoint 2010*" was an ARMA best seller, and the second edition was released in October 2015. Bruce holds a Diploma in Electronics Engineering Technology, a Masters in Business Administration from Queen's University, and is a certified Information Governance Professional. Throughout his career, he has founded 4 companies:

Provenance Systems	World's first electronic records software
Tarian Software	World's first reusable electronic recordkeeping engine
RIMtech	Electronic records education and consulting
Catalyst IG Tools	Specialty EDRMS deployment tools for Microsoft SharePoint

Course Topics

Topic	Description
Sensitive Information Types (SITs)	SITs enable consistent, automated protection of sensitive information, reducing compliance risk. Automatically identify sensitive data such as credit card numbers based on built-in or custom patterns. Learn to classify, label, protect, and govern content by detecting sensitive information. SITs form the foundation sensitivity labels, data loss prevention (DLP), retention, and compliance controls.
Data Profiling	Data profiling enables informed, risk-based decisions, and provides visibility into the types and volumes of sensitive information by analyzing content and identifying patterns such as personal, financial, or confidential data. Identify where sensitive information resides, who is using it, and whether it is adequately protected.
Sensitivity Labels	Sensitivity labels embed protection directly into content, preventing unauthorized access and accidental disclosure. Learn how to mandate labelling when users save, send, or share a document. Learn optimal ways to apply suitable labels automatically, triggering protections such as encryption, access restrictions, content markings, and sharing controls. Automatic labelling improves compliance and reduces human error.
Encryption	Encryption provides persistent protection that remains with the information wherever it travels, helping to prevent unauthorized access and data breaches. Learn when, where, and how to apply encryption either automatically or manually, based on the sensitivity level.
Usage Rights	Usage rights provide granular control over information after access is granted, helping to prevent misuse, unauthorized distribution, and accidental disclosure of sensitive information. Control what authorized users can do with protected content, such as viewing, editing, printing, copying, forwarding, or extracting information, and when such rights can expire.
Email Protection	Classify, encrypt, and apply usage restrictions to email messages based on their sensitivity. Automatically or manually protect emails containing confidential, personal, financial, or regulated information, and control who can read, forward, print, or copy message content, both inside and outside the organization.
Container Labelling	Secure collaboration spaces by applying sensitivity labels to workspaces such as Teams, Groups, and SharePoint. Automatically enforce settings such as privacy levels, external sharing restrictions, unmanaged device access controls, and guest access permissions.
Auto Labeling Policies	Learn to enforce information protection requirements efficiently across large volumes of content. See how to automatically apply sensitivity labels to content when predefined conditions are met, such as the detection of sensitive information types, keywords, trainable classifiers, or metadata values. Classify and protect documents and emails at scale.
Data Loss Prevention	Reduce accidental or nefarious data leaks by automatically blocking, restricting, encrypting, or warning users when protected information is shared inappropriately. Understand DLP lifecycle, policies, and alerts.
Content Marking	Content Marking makes classification immediately visible, supporting compliance and encouraging consistent information handling. Automatically add visual indicators such as headers, footers, and watermarks to documents and emails based on their sensitivity label. Clearly communicate the classification and handling requirements to users, both inside and outside the organization.
Classification Analytics	Learn how to use Content and Activity Explorers to generate insights into how information is being classified, labelled, and protected. Monitor adoption of sensitivity labels, identify sensitive data trends, measure policy effectiveness, and uncover areas of potential risk.
User Justification & Overrides	Allow users to provide a business reason when changing, downgrading, removing, or overriding a sensitivity label or protection policy. This allows flexibility without sacrificing oversight and traceability.
External Sharing Protection	Reducing the risk of data leakage, unauthorized access, and non-compliance with privacy and security requirements. Share sensitive information with external parties while maintaining control over access and usage.
Microsoft Copilot Protection	You'll need to ensure that Microsoft Copilot respects existing sensitivity labels, permissions, encryption settings, and access controls when generating responses or retrieving data. Prevent Copilot from exposing information that users are not authorized to access and ensure that sensitive data remains protected within AI-powered workflows.

Advantages of RIMtech Training

- ✓ **NOT** a feature tour. Practical, real-life deployment training based on actual projects.
- ✓ 100% vendor neutral content. We do not sell Microsoft products or services. We are not tied to Microsoft in any way.
- ✓ Instruction by **Bruce Miller**. Learn from, and interact with, the top expert in electronic recordkeeping.
- ✓ We understand IT AND records management. We speak your language.
- ✓ We simplify complex technology so you can understand it.
- ✓ We have developed Catalyst IG Tools –the world's only specialized tools for EDRMS deployment.
- ✓ Real-world examples and experience from actual projects.
- ✓ The very latest in technology, techniques, and methods.
- ✓ Best practices, developed by RIMtech.
- ✓ Engaging, dynamic, interactive instruction. Exercises to facilitate learning.
- ✓ You get to keep materials and tools following completion.
- ✓ Access to full session recording
- ✓ CRM/IGP/CIP credits for all courses.
- ✓ Official Completion Certificate.

Registration Form (1 form per participant)				Class	PurIP1U
Mr/Ms/Mrs.	Name			Title	
Organization			Dept.		
Address					
City	State/Prov	Zip/PostCode	Country		
Telephone	Email				
Payment Method					
Please Bill Credit Card	☐ Visa	☐ Mastercard	☐ Amex		
Name on Card					
Card Number		Expiry Date (YY/MM/DD)		CCV	
Signature					
☐ Cheque, Payable to RIMtech Inc.	☐ Invoice, P.O. # (Attach P.O.)				

Five Ways to Register & Pay	
Online	Go to the appropriate class page under Training & Education. Select the class, then pay via PayPal or credit card
Telephone	Call Natalie Arruda at 343-572-8533 to give your credit card details over the phone.
Email	Complete this form and scan it to PDF, then email it to us at natalie@rimtechconsulting.com
Cheque	Complete this form and enclose a cheque. Mail to RIMtech Inc., 50 Argue Drive, Ottawa, On Canada K2E 6S1
Purchase Order	Complete this form, include Purchase Order, scan to PDF, then email to us at natalie@rimtechconsulting.com

Microsoft Purview Information Protection	**Price**	
	Regular	**ARMA/AIIM Member**
	US $800	US $700
Applicable Taxes	Outside Canada	none
	AB, SK, BC, MB, NT, QC, NU, YT	5%
	ON	13%
	NB, NL, NS, PE	15%

Technology Requirements

1. Reliable, stable high-speed Internet connection
2. Zoom App available at https://**zoom**.us/**download** (downloads automatically upon first meeting sign-in)
3. Camera optional but recommended

Terms and Conditions

This is a summary only. See https://www.rimtechconsulting.com/terms-conditions for our detailed Terms and Conditions.

1. **Equipment Requirements**. Each participant is responsible for the technology requirements above in order to participate successfully in any RIMtech online class or event.
2. **No Recordings**. Sessions are not recorded, to protect the privacy of participants.
3. **Class Materials**. Participants will receive all class materials in electronic form. Materials will be posted to a restricted page of RIMtech's website for that particular class.
4. **No-Shows.** If a participant fails to attend a class without a notification of cancellation, no refund will be issued. RIMtech will make the class materials available for that participant.
5. **Payment.** Payment, or a Purchase Order, must be received by the class date. All invoices are due within 30 days.
6. **Participant Contact**. We require the name, email addresses, and telephone number of each participant prior to the start of each class.
7. **Participant Substitution**. A participant may be substituted at any time, by contacting natalie@rimtechconsulting.com.
8. **Participant Cancellation**. To cancel, you must notify us 5 days prior to the class date. The class fee will be refunded less a 10% administrative fee. If cancellation is received later than 5 days prior to class start date, participant may nominate a substitution, or RIMtech will issue a credit voucher for the full amount of the class, redeemable for 1 year against any class of equal or lesser value.
9. **RIMtech Cancellation**. RIMtech reserves the right to cancel any class for any reason, such as a failure to reach the minimum class registration size, instructor illness, etc. In such an event, RIMtech shall refund the full registration fee paid. RIMtech will make every effort to notify registrants as soon as possible of any such cancellation.
10. **RIMtech Postponement**. RIMtech reserves the right to postpone/reschedule any class for any reason and will, in such an event, work with registrants to find a mutually acceptable reschedule date. If such a date is not acceptable to any registrant, a full refund will be issued. RIMtech will make every effort to notify registrants as soon as possible of any such cancellation.
11. **Liability**. RIMtech assumes no liability for changes in course dates or content.
12. **Currency**. All fees are in US dollars.

Natalie Arruda natalie@rimtechconsulting.com 343-572-8533
Bruce Miller bmiller@rimtechconsulting.com 613-795-3072