Information protection

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CLASSIFY AND PROTECT

Detect SIT / classifier → **Label** Classification → **Protect** Rights + markings → **Publish** User availability

01 Implement information protection 25-30%

Choose the classification method

- **Sensitive information types (SITs)** recognize structured data such as passport numbers, payment cards, employee IDs and credentials. Reuse a built-in detector before creating a custom one.
- **Regular expressions** recognize a format; **keyword lists and dictionaries** recognize terms. Use a **trainable classifier** for a document category such as resumes, contracts or source code.
- **Exact data match (EDM)** recognizes values from an authoritative dataset. **Document fingerprinting** recognizes a standard form or template, including filled-in copies.
- Classification identifies content. A **sensitivity label** can protect it, **DLP** controls risky use or sharing, and **retention** governs preservation and deletion. These controls can coexist.

Build and test a custom SIT

- A detection **pattern** combines a primary element with optional supporting evidence, character proximity and confidence. A policy separately sets the required confidence and instance count.
- For three letters followed by three digits, use a pattern such as **[A-Za-z]{3}[0-9]{3}**, with suitable boundaries. **^** and **$** anchor the entire input rather than an embedded occurrence.
- Put an employee-number format in the primary element and words such as Employee or ID in supporting evidence. **Proximity** limits how far apart the evidence can occur.
- Use **additional checks or exclusions** to reject known test values. A keyword dictionary can be imported from a prepared text list; a CSV dataset is not automatically an EDM classifier.
- **Test** representative matches, near matches and benign content. Copy an editable built-in SIT when appropriate; tenant administration does not make every built-in detection definition editable.

EDM and document fingerprints

- An **EDM schema** describes the source table fields and searchable elements. The EDM SIT rule package defines primary matches and corroborating fields from the same record.
- Prepare the sensitive source table, define the schema and rule package, then **hash and upload** the dataset with **EdmUploadAgent.exe**. The service receives protected hashes rather than the clear-text source table.
- Authorize upload operators through the **EDM_DataUploaders security group**. Refresh uploaded hashes when the authoritative dataset changes; retain the local source securely.

Information protection

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CLASSIFY AND PROTECT

Detect SIT / classifier → **Label** Classification → **Protect** Rights + markings → **Publish** User availability

- For **document fingerprinting**, connect with **Connect-IPPSSession**, read the template bytes, create a fingerprint with **New-DlpFingerprint**, and create its SIT with **New-DlpSensitiveInformationType**.
- Fingerprint the common blank form rather than collecting a training corpus. A fingerprint detects template structure; EDM checks dataset values; a classifier learns a broader content category.

Trainable classifiers

- Prefer a suitable **pretrained classifier**, such as Resumes or Source code, when it meets the requirement. Create a custom classifier for organization-specific categories.
- Store representative **positive and negative samples** in dedicated SharePoint Online folders. The creator needs access to the seed content; a local share or OneDrive folder is not a substitute.
- Use readable, supported files. Encrypted, low-quality, duplicate or unrepresentative samples weaken training. Seed selection is based on content, not an arbitrary filename sequence.
- Follow **seed -> train -> test -> review predictions -> publish**. Keep independent test examples and review false positives and false negatives before using the classifier in enforcement.
- Use classification review feedback to improve supported classifiers. **Built-in and custom classifiers have different retraining capabilities**; a published category detector is not a regular expression.

Labels, publishing and priority

- A **sensitivity label** defines classification, scope and protection. A **label policy** publishes labels to selected users or groups and sets defaults, mandatory labeling and downgrade justification.
- **Creating**, **publishing** and **applying** a label are separate steps. Restrict a finance label through every policy that publishes it; a second broad policy can still expose it.
- Users receive the available labels from applicable policies. For conflicting policy settings, the **highest-priority applicable policy** wins; this differs from the sensitivity ranking of individual labels.
- Order labels from less sensitive to more sensitive. **Sublabels** carry their own configuration; a parent with sublabels is a category, so choose an applicable sublabel as the default.
- **Default labeling** supplies an initial choice. **Mandatory labeling** requires a label. Neither means that every item must use one specific label or that a label grants permission to open encrypted content.

Information protection

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CLASSIFY AND PROTECT

Detect SIT / classifier → **Label** Classification → **Protect** Rights + markings → **Publish** User availability

Encryption and content markings

- **Azure Rights Management** supplies label-based encryption and usage rights. Configure either administrator-defined permissions or supported user-defined permissions when the label is applied.
- **Label availability** and **content authorization** are independent. A recipient can be authorized to read an encrypted file without being allowed to apply that label to new content.
- **Any authenticated users** permits supported authenticated identities to open the encrypted content without restricting access to your organization. Use specific users or groups when recipient access must be limited.
- **Headers, footers and watermarks** are visual markings, not access controls. Watermarks apply to supported documents; email supports headers and footers. Labeling an email does not stamp markings into its attachments.
- Distinguish **content expiry** from the **offline access/use-license period**. Cached rights and reauthorization affect when changes are enforced; editing a label does not simply restart every document's original clock.
- Encrypted-file **co-authoring** needs tenant enablement and compatible apps. **Double Key Encryption** and expiring content access restrict co-authoring; user-defined permission support depends on the client configuration.

Automatic and container labeling

- **Client-side auto-labeling** recommends or applies a label while a user works in a supported Office app. **Service-side auto-labeling** inspects supported SharePoint/OneDrive files at rest and Exchange email in transit.
- Run service-side policies in **simulation**, inspect matches, refine conditions and then enable application. Simulation discovers prospective matches without applying the label.
- Label replacement depends on **existing label priority and application method**. Do not assume an automatic policy will overwrite a manually chosen label or label an attachment as a separate file.
- Enable **sensitivity-label integration for SharePoint and OneDrive** for supported web and service processing. **Groups & sites** scope controls container privacy, external sharing and access settings; it does not label every contained document.
- The **Microsoft Purview Information Protection scanner** discovers, classifies and protects supported on-premises repositories using a scanner cluster and content scan job. Use repository permissions and a discovery run before enforcement.

Information protection / Data loss prevention

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CLASSIFY AND PROTECT

Detect SIT / classifier → **Label** Classification → **Protect** Rights + markings → **Publish** User availability

Message encryption and mail flow

- **Microsoft Purview Message Encryption**, also called **OME**, uses Azure Rights Management. **Encrypt-Only** encrypts a message; **Do Not Forward** additionally restricts recipient usage.
- Use an **Exchange mail flow rule** for conditions such as recipient domain, attachments or sensitive information. Use an eligible published sensitivity label for a user's manual encryption choice.
- **Advanced Message Encryption** adds custom branding and supported portal-message expiration and revocation. Create a branding configuration with **New-OMEConfiguration**, then select it through the applicable mail flow action.
- Revocation depends on the **message delivery and recipient experience**. Use the supported revocation action or **Set-OMEMessageRevocation** for eligible portal messages; deleting a Sent Items copy does not revoke recipient access.
- Use **Test-IRMConfiguration** to test templates and encryption/decryption. **TLS connectors** enforce protected server-to-server transport and certificate validation; persistent message rights are a separate protection layer.
- Attachment protection depends on **format, existing protection and encryption mode**. Supported Office attachments can inherit rights; an encrypted email does not make every attachment format independently rights-managed.

02 Implement DLP 15-20%

DLP policy design

- A **DLP policy** selects locations and populations. Its rules combine conditions, exceptions and actions, with user notifications, override choices and administrator alerts configured separately.
- Select locations from the **actual data path**: Exchange for email, SharePoint/OneDrive for files, Teams for messages and Devices for endpoint activity. Available conditions and actions vary by location.
- Use **Content contains** with SITs, labels or supported classifiers. Set **instance count**, confidence and external-sharing conditions to distinguish one identifier from a bulk disclosure.
- Policies that span workloads expose their supported condition set. Split policies when a required action or location combination cannot be expressed together; do not infer a policy count from the number of SITs.
- Apply narrow **scope exclusions or rule exceptions** for an authorized business group. Keep other locations and rules enforced rather than disabling the whole policy.

Data loss prevention

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CONTROL SENSITIVE-DATA ACTIVITY

Scope Data locations → **Detect** Rule conditions → **Act** Audit / restrict → **Review** Matches + alerts

Actions, tips and precedence

- **Block external sharing** differs from restricting access for everyone. A SharePoint DLP restriction can preserve access for designated owners or administrators; it is not file encryption.
- **Policy tips** educate the user at the supported point of use. **Email notifications**, **incident reports** and **administrator alerts** have different audiences and configuration.
- A permitted **override** can require a business justification or false-positive report. Review the **False positives and overrides** report to understand these decisions.
- Interpret **policy priority, rule priority, stop-processing settings and workload behavior** together. Several rules can match, while the resulting restriction or displayed policy tip may differ from the full match list.
- Use **simulation/test mode** before enforcement. Tune detections from observed matches; raise an **alert aggregation threshold** to reduce notification volume without weakening the underlying content match.

Teams messages and shared files

- **Teams chat and channel messages** covers message content. Sensitive text can be blocked or removed from the recipient experience with a DLP policy scoped to Teams.
- Files shared in **chats** reside in the sharer's **OneDrive**. Files shared in **channels** reside in **SharePoint**. Protect those file locations in addition to the Teams message location.
- A Teams message policy does not automatically secure every linked file. **Private and shared channels** can use separate SharePoint sites, so include the actual backing sites.
- Scope policies to the intended users, teams and file locations. A file's DLP evaluation and a message's evaluation occur through their respective workloads.

Endpoint DLP deployment and actions

- Enable **device onboarding** in Purview and onboard supported devices. Devices already onboarded to **Microsoft Defender for Endpoint** can be available through the shared onboarding integration.
- Use an appropriate deployment method such as **Intune, Group Policy, Configuration Manager or a local script**. Device enrollment or Entra join alone does not establish Endpoint DLP monitoring.

Data loss prevention

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

CONTROL SENSITIVE-DATA ACTIVITY

Scope Data locations → **Detect** Rule conditions → **Act** Audit / restrict → **Review** Matches + alerts

- Select **Devices** in the DLP policy. Match sensitive content or labels and configure activities such as **USB copy, clipboard copy, printing, network-share copy and upload**.
- Activity actions include **Audit only**, **Block with override** and **Block**, where supported. Audit records an action while allowing it; the action setting determines enforcement.
- Validate the **OS, application, browser and file-type support** for the activity. Being onboarded to Defender does not mean every device platform supports every Endpoint DLP control.

Endpoint settings and cloud apps

- **Service domains** control sensitive uploads to selected destinations. In **Allow** mode, listed destinations form the permitted set; in **Block** mode, listed destinations form the restricted set.
- **Unallowed/restricted apps** target local executables accessing sensitive files. **Unallowed browsers** prevent unsupported upload paths; supported browser extensions provide additional inspection coverage.
- **File path exclusions** remove matching content from Endpoint DLP monitoring. Use them for an intentional folder exclusion, not to stop one application from reading only sensitive files.
- In **Defender for Cloud Apps**, a **file policy** inspects stored content, labels and sharing. An **activity policy** detects actions such as an upload; an **app discovery policy** discovers cloud app usage.
- Separate **alerts** from **governance actions** such as quarantine or labeling. Remove a quarantine action to retain alerting without quarantine. Use supported **Power Automate** integration for custom routing.

Monitor and investigate DLP

- **DLP policy matches** reports show rule and policy detections. **DLP incidents** and the alert queue support investigation; not every rule match has to generate an administrator alert.
- Use **Activity explorer** to filter rule matches, endpoint activity and label changes. Expand event details to inspect detected information and export the relevant activity data.
- Inspect the **matched rule, sensitive information, affected item, user and action** before classifying an alert. Resolve, dismiss or escalate according to the alert type and available workflow.
- Grant **DLP administration, alert reading and content investigation** independently through Purview RBAC. Downloading message evidence needs appropriate content-investigation permissions beyond a read-only alert view.

Retention & records

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

GOVERN THE CONTENT LIFECYCLE

Apply Policy / label → **Preserve** Retention clock → **Review** Disposition → **Dispose** Eligible content

03 Implement data lifecycle and records management 10-15%

Retention policies and labels

- A **retention policy** applies common lifecycle settings to selected locations. A **retention label** applies item-level settings and can declare a record. One item has one retention label, alongside applicable policies.
- Choose **retain only**, **retain then delete**, or **delete only**. Retention can preserve a hidden copy after user deletion; it does not always prevent the user from deleting the visible item.
- **Publish labels** to make them available for users or library defaults. **Auto-apply labels** to match SITs, supported classifiers, keywords or searchable properties; publication alone does not classify every item.
- Set the retention clock from **creation, last modification, labeling or an event**, as supported. A duration without its start condition is insufficient to calculate expiry.
- Use an **auto-apply query** for searchable metadata or keywords. Search query syntax is not a general regular-expression engine; use a SIT for a structured identifier in content.

Scopes and workload coverage

- A **static scope** lists included and excluded locations. An **adaptive scope** evaluates supported user, site or group attributes so membership can change as the organization changes.
- Use attribute-based site selection for recurring departmental sites. Choose the **scope object type** that matches the target location; a user scope and a Microsoft 365 group scope select different resources.
- **Teams message retention** is configured separately from general Exchange/SharePoint retention. Retain the backing **SharePoint and OneDrive** locations for channel and chat files.
- A **Microsoft 365 group** has a mailbox and associated site. Private/shared channel sites and other connected resources may need their own coverage; selecting the team name is not proof that all content is retained.
- A **cloud-attachment retention label** can preserve the supported shared version of a linked file. Scope the originating Exchange or Teams sharing activity and the attachment-label workflow correctly.

Retention & records

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

GOVERN THE CONTENT LIFECYCLE

Apply Policy / label → **Preserve** Retention clock → **Review** Disposition → **Dispose** Eligible content

Retention conflicts and preservation

- For ordinary overlapping retention settings, **retain wins over delete** and the **longest applicable preservation requirement** wins. A deletion deadline cannot release content still preserved by another requirement.
- After preservation requirements are satisfied, **explicit deletion settings take precedence over implicit settings**. A label's delete action takes precedence over a policy's; remaining deletion conflicts use the applicable shortest expiry.
- Calculate **actual end dates**, not just the largest number of years. Creation-based and modification-based clocks can yield different expiry dates; use **Policy lookup** to identify assigned settings.
- SharePoint/OneDrive can retain deleted or changed content in the **Preservation Hold Library**. Exchange preserves eligible deleted content in **Recoverable Items**; neither is the user's ordinary visible folder.
- Retention and cleanup run asynchronously. A recycle bin, OneDrive deleted-user retention and compliance retention serve different purposes; user-account deletion does not automatically release preserved content.

Records and file plans

- Declare content as a **record or regulatory record with a retention label**. A sensitivity label controls protection and does not declare a compliance record.
- A **standard record** supports controlled lock/unlock behavior. With record versioning, **unlock -> edit -> lock** preserves the previous record version while allowing the authorized update.
- A **regulatory record** imposes stricter immutability: its label cannot be removed, and content changes and deletion are restricted. Read/copy and moves within the supported container remain possible.
- Expose regulatory-record labeling with **Set-RegulatoryComplianceUI -Enabled $true** after **Connect-IPPSSession**. Regulatory-record labels use publication/application rather than automatic labeling.
- A **file plan** catalogs retention labels and descriptors such as business function, category and authority. **CSV import/export** supports bulk label management; importing a file plan does not publish the labels.

Retention & records

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

GOVERN THE CONTENT LIFECYCLE

Apply Policy / label → **Preserve** Retention clock → **Review** Disposition → **Dispose** Eligible content

Events, disposition and locks

- **Event-based retention** starts a label's clock from a business event such as contract termination or fiscal-year close. Configure the label's **event type**, label the content and identify the related assets.
- Create the event with its **event date and asset IDs or query** to target the intended content. Files awaiting the event remain preserved; file creation is not the event's retention start.
- At period end, a label can **delete, start disposition review, change the label or run a Power Automate flow**, as supported. A flow can implement custom processing such as moving a file.
- **Disposition review** routes items through assigned reviewers and stages. **Disposition Management** permissions and reviewer assignment are separate from merely administering a SharePoint site.
- **Preservation Lock** prevents even global administrators from disabling, deleting or weakening a policy. Retention periods and locations can be expanded; adaptive scopes do not support the lock.
- Use **Set-RetentionCompliancePolicy -RestrictiveRetention $true** for the irreversible policy lock. A locked label policy must publish only **regulatory-record labels**; labels may be added, not removed.

Mailbox holds, archives and recovery

- Use **Get-Mailbox** to inspect **LitigationHoldEnabled, InPlaceHolds** and related retention-hold properties. Also check organization-wide holds with **Get-OrganizationConfig** when determining why a mailbox is preserved.
- **Litigation Hold, eDiscovery hold and Purview retention** preserve content. Exchange **RetentionHoldEnabled** pauses MRM processing; that setting alone does not create a legal preservation hold.
- **Exchange MRM retention tags and policies** control actions such as **Move to Archive**. Use **Start-ManagedFolderAssistant** to request processing. A Purview retention label does not move email to an archive mailbox.
- Removing an MRM tag from a policy stops offering it through that policy; already tagged items can continue to be processed. Deleting the tag is a different administrative operation.
- Use **Get-RecoverableItems** and **Restore-RecoverableItems** for eligible deleted messages. For an **inactive mailbox**, recover into a new mailbox or use **New-MailboxRestoreRequest** to copy content into an existing mailbox.
- Place the required preservation hold before deleting a departing user's account to retain an eligible inactive mailbox. Recovery depends on the retained mailbox state, not restoring a directory account alone.

Monitoring & investigation

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

COLLECT EVIDENCE AND INVESTIGATE

- **Content explorer** — Classified items
- **Activity explorer** — Data actions
- **Audit** — Recorded events
- **eDiscovery** — Search + holds

04 Monitor and investigate data and activities 15-20%

Content, activity and permissions

- **Content explorer** shows where classified items are located. **Activity explorer** shows actions such as label changes and DLP matches. **Audit search** investigates recorded user and administrator operations.
- **Content Explorer List Viewer** permits the item list; **Content Explorer Content Viewer** permits opening content. Administrative access to a solution does not automatically grant access to sensitive content.
- Use **Sensitivity label administrator** or appropriate information-protection permissions for label management. Use separate retention, DLP, audit and investigation roles for their respective tasks.
- Assign **Purview role groups** for compliance workloads and the smallest practical scope. **Role Management** governs role assignments; licensing enables features but does not grant investigation permissions.

Audit search and retention

- **Audit (Standard)** provides unified audit collection and search. **Audit (Premium)** adds capabilities such as extended retention and additional high-value events for eligible licensed users.
- An **audit retention policy** selects users, record types, activities, retention duration and priority. A higher-priority custom match can determine the result; the longest configured policy does not automatically win.
- Long retention depends on the license of the **user generating the event**. A **10-year audit retention add-on** assigned only to the administrator does not extend everybody else's records.
- Use **Audit Reader/View-Only Audit Logs** for appropriate read-only searches. Confirm collection, time range, workload, activity and ingestion delay when expected events are missing.
- **Mailbox auditing**, **administrator auditing** and mailbox permissions are different controls. Granting folder access does not enable missing mailbox events; enabling auditing cannot recreate uncollected history.
- An **alert policy** detects selected audit activities, including investigation or administrative actions. Configure aggregation, severity and recipients; changing an alert's status does not change its detection rule.

eDiscovery, searches and holds

- **eDiscovery (Standard)** provides case-based search, export and holds. **Premium** adds capabilities such as custodians, collections, review sets and analytics for a more extensive investigation workflow.
- An **eDiscovery Manager** works with permitted cases. **Case membership** controls access to a particular case; an **eDiscovery Administrator** has broader case access. Mailbox Send As permission is unnecessary for compliance searching.
- Use **KQL property restrictions**, explicit **AND/OR** and parentheses for recipients, sender, dates and keywords. A trailing wildcard supports eligible prefix searches; KQL is not regular-expression matching.

Monitoring & investigation / Insider & privacy risk

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

COLLECT EVIDENCE AND INVESTIGATE

- **Content explorer** — Classified items
- **Activity explorer** — Data actions
- **Audit** — Recorded events
- **eDiscovery** — Search + holds

- A **search** finds content. A **case hold** preserves scoped content, optionally filtered by a query. Export needs the relevant export permissions and workflow; preview is not the full exported dataset.
- Use **Get-UnifiedGroup** to identify a Microsoft 365 group's mailbox and site. Preserve the actual backing resources for Teams content; cloud eDiscovery does not directly search an on-premises mailbox merely because its identity is synchronized.

Compliance Manager assessments

- A regulatory **template** defines controls. An **assessment** evaluates an implementation against those controls. Use the relevant assessment for GDPR or an ISO standard; the **Data Protection Baseline** is a separate starting point.
- **Improvement actions** describe work, owners, implementation status, evidence and testing. Distinguish **Microsoft-managed** actions from customer responsibilities and manual testing from automatic testing.
- For a manual action, implement the control, record evidence and update the **test status/result**. Setting only Implementation status to Implemented does not necessarily award compliance-score credit.
- **Reader** views data; **Contribution** edits data and creates assessments; **Assessor** edits assessment data; **Administration** manages templates, tenant data and assignments. Scope assessment access to the intended work.
- Use **assessment groups**, solution/control filters and assessment alerts to organize related work and changes. A score measures assessed progress rather than certifying legal compliance; template availability depends on the subscription entitlement.

05 Manage insider and privacy risk in Microsoft 365 15-20%

Communication compliance

- **Communication compliance** detects and reviews business-conduct or regulatory issues in communications, including harassment, threats, conflicts of interest and sensitive information. It supports investigation and remediation.
- Define **monitored users/groups, locations, conditions, sampling and reviewers**. Exchange and Teams are common sources; supported Viva Engage and third-party content require the appropriate integration.
- Use **SITs** for structured secrets and personal data, and suitable **classifiers** for language or contextual categories. A policy to detect insider stock information is different from a barrier that blocks all communication.

Insider & privacy risk

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

MATCH THE RISK TO THE CONTROL

- **Communications** — Review conduct
- **Insider risk** — Correlate signals
- **Barriers** — Limit collaboration
- **Priva** — Personal data

- **Pseudonymization** controls identity display. **Sentiment analysis** supplies positive, neutral or negative context; it is not itself a final finding of misconduct.
- Review alerts, inspect permitted message context, tag findings and remediate or escalate. Notification templates support consistent user guidance; third-party sources such as Zoom require supported **data connectors**.

Separate administration from review

- **Communication Compliance Administrators** configure policies and solution settings. That administrative role does not itself permit investigating message alerts.
- **Communication Compliance Analysts** investigate and perform permitted triage. **Investigators** have additional remediation and message-detail/export capabilities. **Viewers** access reporting rather than message investigations.
- **Insider Risk Management Admins** configure policies. **Analysts** triage alerts; **Investigators** work with cases and investigation content. Grant evidence access only to those who need it.
- Policy **reviewer assignment**, solution role membership and evidence permissions are distinct gates. Use the task-specific role rather than broad global administration for every compliance task.

Insider risk signals and templates

- **Insider risk management** correlates user activity with triggering events and risk indicators. Choose a template for **data leaks, departing-user theft, security policy violations** or another supported scenario.
- An **HR data connector** supplies signals such as resignation, termination or performance changes. Prepare mapped **CSV** data and the required application/connector permissions; an Office indicator alone does not supply an HR event.
- Enable the required **Office, device and other indicators**. Onboard supported devices to Purview to observe activities such as sensitive-file deletion, USB copying or printing.
- **Priority user groups** focus elevated-risk policy treatment on sensitive populations. **Analytics** identifies patterns for policy planning; enabling analytics alone does not deploy a targeted enforcement policy.
- Set **activation and historical detection windows** for the template, then triage alerts into cases. A triggering event, policy scope and enabled indicators all affect what activity contributes to risk.

Insider & privacy risk

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

MATCH THE RISK TO THE CONTROL

- **Communications** — Review conduct
- **Insider risk** — Correlate signals
- **Barriers** — Limit collaboration
- **Priva** — Personal data

Adaptive Protection and evidence

- **Adaptive Protection** uses insider-risk levels to adjust protection through supported controls such as DLP. Risk-based policy treatment connects user context with sensitive-data controls.
- **Forensic evidence** captures visual clips of supported security-related device activity for an investigation. It is separate from the audit events used for ordinary activity reporting.
- Configure forensic-evidence **capacity, permissions, capturing policies and supported device onboarding** before capture. Purview onboarding for another feature does not prove the capture prerequisites are complete.
- Use **notice templates**, privacy controls and restricted evidence access as part of the investigation workflow. Review the specific feature's supported device platform rather than assuming all Endpoint DLP platforms can capture clips.

Information barriers

- **Information barriers (IBs)** prevent prohibited communication and collaboration between populations. A **segment** is defined by supported user attributes and a **user group filter**; it is not just a security-group membership list.
- Create segments with **New-OrganizationSegment**, define allow/block policies with **New-InformationBarrierPolicy**, activate them and start policy application. Check application status after configuration.
- Use **Get-InformationBarrierRecipientStatus** to inspect a user's applied IB status. Check authoritative user attributes when one person is outside the intended segment while the policy works for others.
- Apply the appropriate **SharePoint/OneDrive IB mode and segment association** for collaboration. Supported site settings, tenant enablement and user compatibility work together with Teams enforcement.
- **Single-segment and multi-segment modes** have different membership capabilities. Check the tenant mode and intersecting policies before assuming a user can belong to several segments or collaborate across them.

Insider & privacy risk

Microsoft Information Protection Administrator

KNOWLEDGE CHEATSHEET

MATCH THE RISK TO THE CONTROL

- **Communications** — Review conduct
- **Insider risk** — Correlate signals
- **Barriers** — Limit collaboration
- **Priva** — Personal data

Priva privacy risk and requests

- **Microsoft Priva Privacy Risk Management** discovers and manages personal-data risk. **Subject Rights Requests** supports responding to a person's request for their data; the capabilities have separate licensing and workflows.
- **Data overexposure** detects personal data exposed too broadly, such as public SharePoint/OneDrive access. **Data transfers** evaluates movement between users, departments, regions or external recipients.
- **Data minimization** detects personal data kept longer than needed or left unused. Match the template to exposure, movement or stale storage rather than treating every external-sharing scenario identically.
- Use **Data profile** to review personal-data locations and detected types. Configure policy scope, conditions, notifications and supported Teams tips; test a policy before active alerting.
- For a **subject rights request**, define the subject's identifying information, request type and supported search locations; collect, review and prepare the response with assigned reviewers and approvers.
- Separate **Privacy Management administration, analysis, investigation and viewing** permissions. Viewing match metadata differs from opening source content or managing request approvers.