# SC-400 Cheat Sheet

**1. Data Classification:**

* **Sensitive Info Types:** Identifies and classifies sensitive information like financial, medical, or personal data. Key for data protection and compliance.
* **Custom Sensitive Info Types:** Customize detection patterns to identify unique organizational data, enhancing targeted protection strategies.
* **Trainable Classifiers:** AI-driven tools that learn to categorize data based on examples. Useful for sorting large volumes of unstructured data.
* **Custom Trainable Classifier:** Create organization-specific classifiers for specialized data types, improving accuracy in data categorization.
* **Exact Data Match (EDM):** Uses a secure hash to match sensitive information against a database, enhancing precision in data protection.
* **EDM Upload Tool:** Facilitates the secure upload of sensitive data hashes to Microsoft 365 for EDM-based classification.
* **Data Classification Service:** Centralizes data classification across Microsoft 365, integrating with various compliance tools.

**2. Data Loss Prevention (DLP):**

* **Data Loss Prevention Policy:** Policies to prevent unauthorized access or sharing of sensitive data, pivotal for regulatory compliance.
* **Endpoint DLP Policies:** Applies DLP controls to endpoint devices, extending data protection beyond the corporate network.
* **Microsoft 365 Endpoint Data Loss Prevention:** Integrates DLP across Microsoft 365 services for a holistic approach to endpoint data security.
* **DLP Policy Matches:** Monitoring these matches is essential for policy refinement and understanding data flow.

**3. Policy Management:**

* **Sensitivity Labels:** Classify and protect content based on its sensitivity, driving encryption, access control, and content marking.
* **Retention Policies:** Controls the lifecycle of information, ensuring data is retained or deleted according to legal or policy requirements.
* **Auto-Labeling Policy:** Uses content analysis to automatically apply sensitivity labels, reducing manual workload and ensuring consistency.
* **File Policy:** Govern and secure file storage and transfer within the organization.
* **Mail Flow Rule:** Manage and secure email routing, vital for data loss prevention and compliance.

**4. Identity Protection and Access Management:**

* **Azure Active Directory (Azure AD) Identity Protection Policies:** Mitigate identity-based security risks through automated detection and response.
* **Identity Protection Policy:** Protects user identities from compromise, a cornerstone of modern security strategies.
* **Conditional Access Policy:** Controls access based on user, location, device status, etc., essential for implementing a zero-trust approach.

**5. Additional Tools and Features:**

* **Custom Branding Template:** Enhances corporate identity and user experience in Microsoft 365, also reinforcing security awareness.
* **Service Domains:** Understand the implications of service domains on configuration and security in the Microsoft cloud ecosystem.
* **Unallowed Apps:** Manage and monitor unauthorized applications to mitigate security risks associated with unsanctioned software.
* **Insider Risk Policy:** Detects and manages internal threats, integrating with analytics and user behavior patterns.
* **Microsoft Defender for Endpoint:** Provides comprehensive endpoint security, crucial for detecting and responding to advanced threats.

# Regular expression cheat sheet (needed for custom DLP rules)

Calculator @ https://regex101.com/

1. **Basic Characters:**
   * **a**, **1**, etc.: Matches exactly the character 'a', '1', etc.
2. **Special Characters:**
   * **.**: Matches any single character except newline **\n**.
   * **\**: Escapes a special character (e.g., **\.** matches a literal period).
3. **Character Classes:**
   * **[abc]**: Matches any one of the characters a, b, or c.
   * **[^abc]**: Matches any character not in the specified set.
   * **[a-z]**: Matches any lowercase letter.
   * **[A-Z]**: Matches any uppercase letter.
   * **[0-9]**: Matches any digit.
4. **Predefined Character Classes:**
   * **\d**: Matches any digit (equivalent to **[0-9]**).
   * **\D**: Matches any non-digit.
   * **\w**: Matches any word character (letters, digits, underscores).
   * **\W**: Matches any non-word character.
   * **\s**: Matches any whitespace character (spaces, tabs, line breaks).
   * **\S**: Matches any non-whitespace character.
5. **Quantifiers:**
   * **\***: Matches 0 or more occurrences of the preceding element.
   * **+**: Matches 1 or more occurrences of the preceding element.
   * **?**: Makes the preceding element optional (0 or 1 occurrence).
   * **{n}**: Matches exactly n occurrences of the preceding element.
   * **{n,}**: Matches n or more occurrences of the preceding element.
   * **{n,m}**: Matches between n and m occurrences of the preceding element.
6. **Anchors:**
   * **^**: Matches the start of a string.
   * **$**: Matches the end of a string.
7. **Groups and Ranges:**
   * **(abc)**: Matches the exact sequence "abc".
   * **|**: Works as an OR operator. For example, **(a|b)** matches either "a" or "b".
8. **Lookahead and Lookbehind:**
   * **(?=...)**: Positive lookahead. Asserts that what immediately follows the current position in the string is **...**.
   * **(?!...)**: Negative lookahead. Asserts that what immediately follows the current position in the string is not **...**.
   * **(?<=...)**: Positive lookbehind. Asserts that what immediately precedes the current position in the string is **...**.
   * **(?<!...)**: Negative lookbehind. Asserts that what immediately precedes the current position in the string is not **...**.