INFORMATION GOVERNANCE CHECKLIST FOR COLLABORATION

CREATED BY
Aware

OWNER
Legal

ADMIN
Human Resources

ADMIN
Infosecurity

EDITOR
Operations

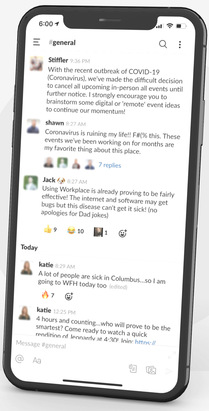
EDITOR
Compliance

Define Data Access

- Involve the right stakeholders. The list often includes the collaboration platform owner, infosecurity, compliance and legal leaders.
- Define levels of access for communication data: Who can adjust records retention policies? Who can search and extract public or private messages? Who is in charge of data loss prevention management?

Reduce Shadow IT

- Understand where employees are collaborating. Be sure to consider both endorsed and shadow solutions.
- Define endorsed tools based on employee needs and the organization's ability to implement securely and quickly.
- Create (or modify existing) acceptable use policies for any newly sanctioned tools.
- Proactively communicate endorsed tools and policies to employees.



Refine Your Information Governance & Enrichment Strategy

- Assess the organization's ability to handle the unique characteristics of collaboration data, including edits, deletions, private messages/hidden conversations, as well as files and attachments.
- Understand where collaboration data is stored (including any data backups or archives).
- Define how your organization's records management policy applies to public and private communications, as well as direct chat in the digital workplace.
- Identify your ability to set dynamic retention policies that align with your records management policies, while also preserving important business context. Confirm your ability to purge data from the collaboration platform and any corresponding archives.
- Consider data enrichment technologies that apply metadata to messages for easy searchability, as appropriate for collaboration conversations. Applicable metadata could include modifications, deletions, message has attachment (define type) and includes images. Also consider additional AI/ML metadata.

Address Regulatory & Compliance Obligations

Outline procedures to satisfy Data Subject Access Requests, as outlined by Article 15 of the GDPR.

Outline procedures to satisfy additional privacy requests, as outlined by the GDPR and CCPA, such as the right to be forgotten.

Identify a rules-based solution to find and remove accidental sharing of PHI/PII/PCI and other confidential information, in order to comply with regulations like HIPAA, FINRA and others.

Streamline Legal & eDiscovery Workflows

Review the Electronic Discovery Reference Model (EDRM) framework to understand the standards for discovery for electronically stored information.

Identify a solution to create an immutable archive of conversation content, including context, that preserves edits and deletions.

Develop a strategy to create and release legal holds, across all endorsed collaboration platforms.

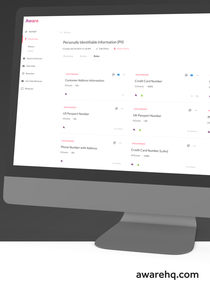
Assess efficient eDiscovery options to quickly filter through conversation data. Consider the ability to look for @mentions, as well as the ability to export messages and message context.

Understand your ability to leverage topics and big-data analysis to surface case analytics, participants and/or groups

Satisfy Your Information Governance Needs with 1 Out-of-the-Box Solution

Time is not a luxury for IT departments in today's pandemic. That's why Aware's turn-key solution quickly addresses risk concerns in collaboration tools like Slack, Microsoft Teams, Yammer and Workplace from Facebook while allowing daily operations and workforce collaboration to continue forward.

Learn About Aware's Remote Work Solutions



Aware

awarehq.com