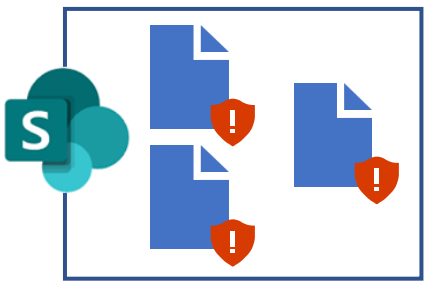
SharePoint sites for highly regulated data with Microsoft 365 for enterprise

A SharePoint site for highly regulated data with Microsoft 365 for enterprise combines the built-in features and security of a private SharePoint team site with additional access restrictions, retention labels, Data Loss Prevention (DLP) policies, and sensitivity labels.

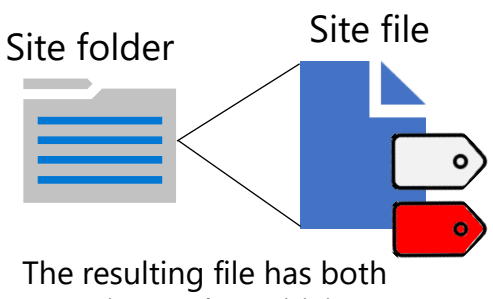
The result is a document collaboration and content management space for your most confidential data with protection that travels with the files you store there.



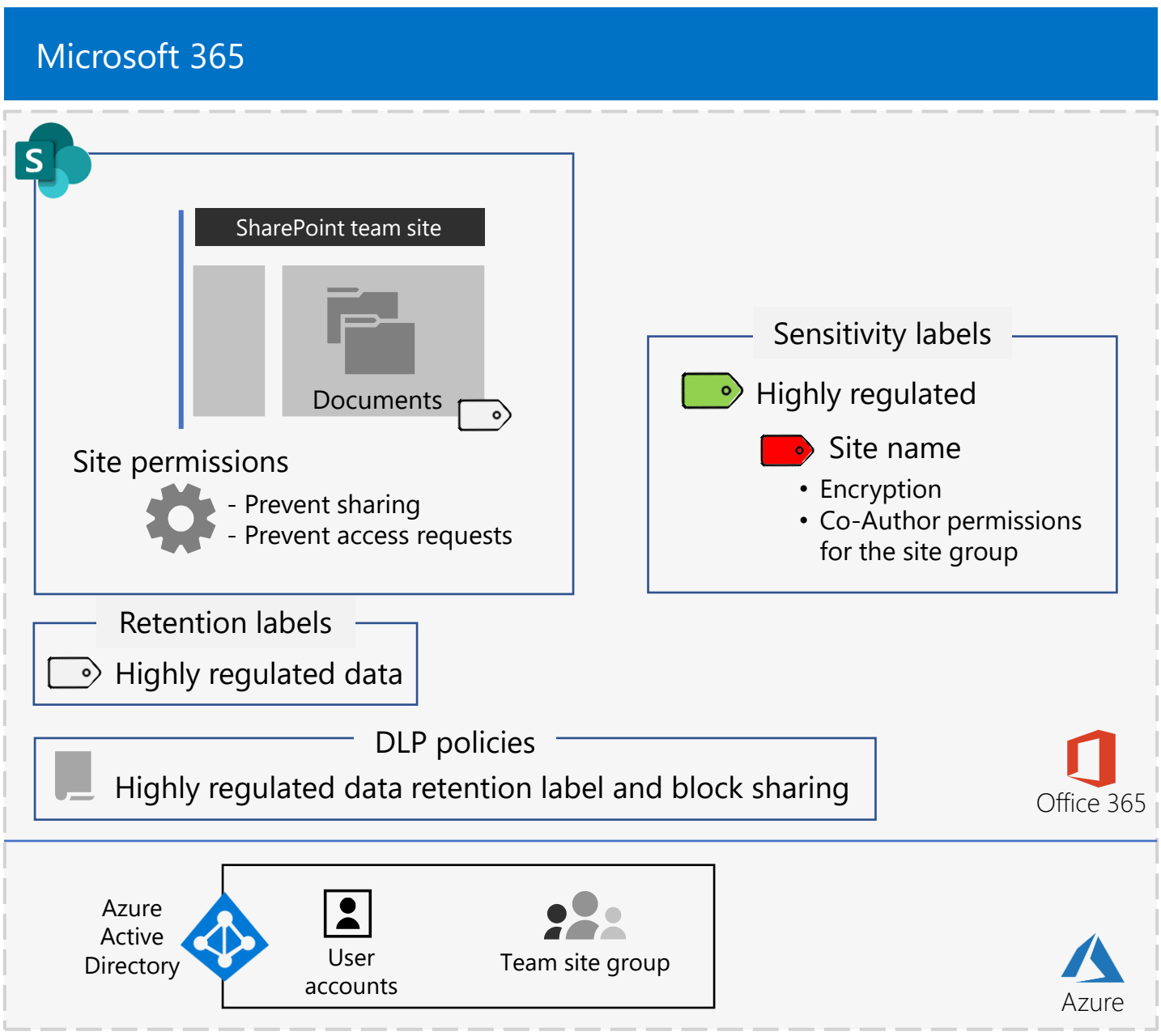
Configuration

	Site permissions and restrictions
	Retention label for highly regulated data
	DLP policy for the highly regulated retention label and to block sharing
	Sensitivity label or sublabel for the site

After the site and these settings and components are in place, a site member creates files in a site folder and applies the sensitivity label or sublabel.



The resulting file has both retention and sensitivity labels applied.



End-to-end deployment using a sublabel

Phase 1: Design

- Implement identity and device access policies.
- Define the purpose of the team site.
- Determine the team site owners and members.
- Define retention label and DLP policy settings.
- Define sensitivity sublabel settings.

Phase 2: Configure

- Create the private team site.
- Configure site owners and members.
- Configure additional team site restrictions.
- Create the retention label and DLP policy.
- Assign the retention label to the documents section of the site.
- Create the sensitivity sublabel.

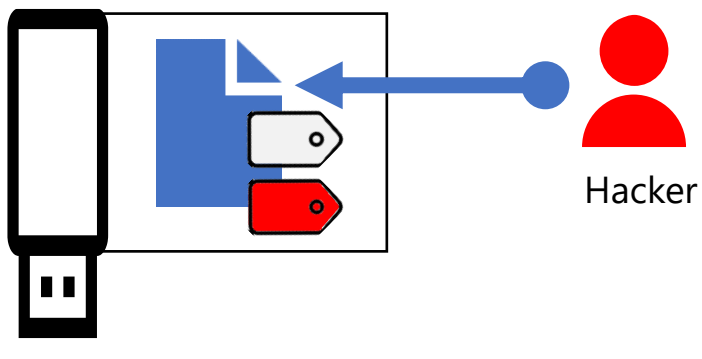
Phase 3: Drive adoption

- Train the team site owners and members on how to use the site, the documents section, and the sublabel.
- Conduct periodic reviews of team site and sublabel usage.
- Retrain as needed.

When a file leaves the site

Contrary to their training, a site member downloads a copy of a file with the sensitivity sublabel assigned and stores it on a thumb drive.

The thumb drive is lost and ends up with a hacker.



When the hacker tries to:

View the file contents.	They can't. The file contents are encrypted.
Open the file using the file's app.	The app prompts the hacker to sign in with credentials.

For deployment guidance, visit aka.ms/m365esecuresites