

Managing Data Security and Governance in SharePoint® and Microsoft 365™

1 Identify Red Flag Risks

Identify Risks:

Identify compliance and security risks, sensitive content types, and access permissions for users and groups.

Involve Stakeholders:

Bring stakeholders such as senior management, IT, information security, privacy and compliance officers, human resources and business units together to conduct a risk assessment and to suggest policies for the organization.

2 Execute the Security Strategy

Establish and Implement a Data Security & Compliance Strategy:

First, use stakeholder knowledge to define your policies and procedures against the business strategy.

Then, automate discovery, classification and policy enforcement to proactively mitigate risk with archTIS's NC Protect™ and Spirion Sensitive Data Platform (SDP) solutions.

3 Implement Products & Design Policies

Design Policies:

Define policies, business rules, policy officers, access rules, notifications and workflows using Spirion SDP and NC Protect.

Map Attributes:

Map available attribute sources in NC Protect including, Entra ID attributes, User Profile Services, company databases, address books, to extract information such as department, employment status, clearance levels, team membership, country, and citizenship to use in dynamic attribute-based access control policies.

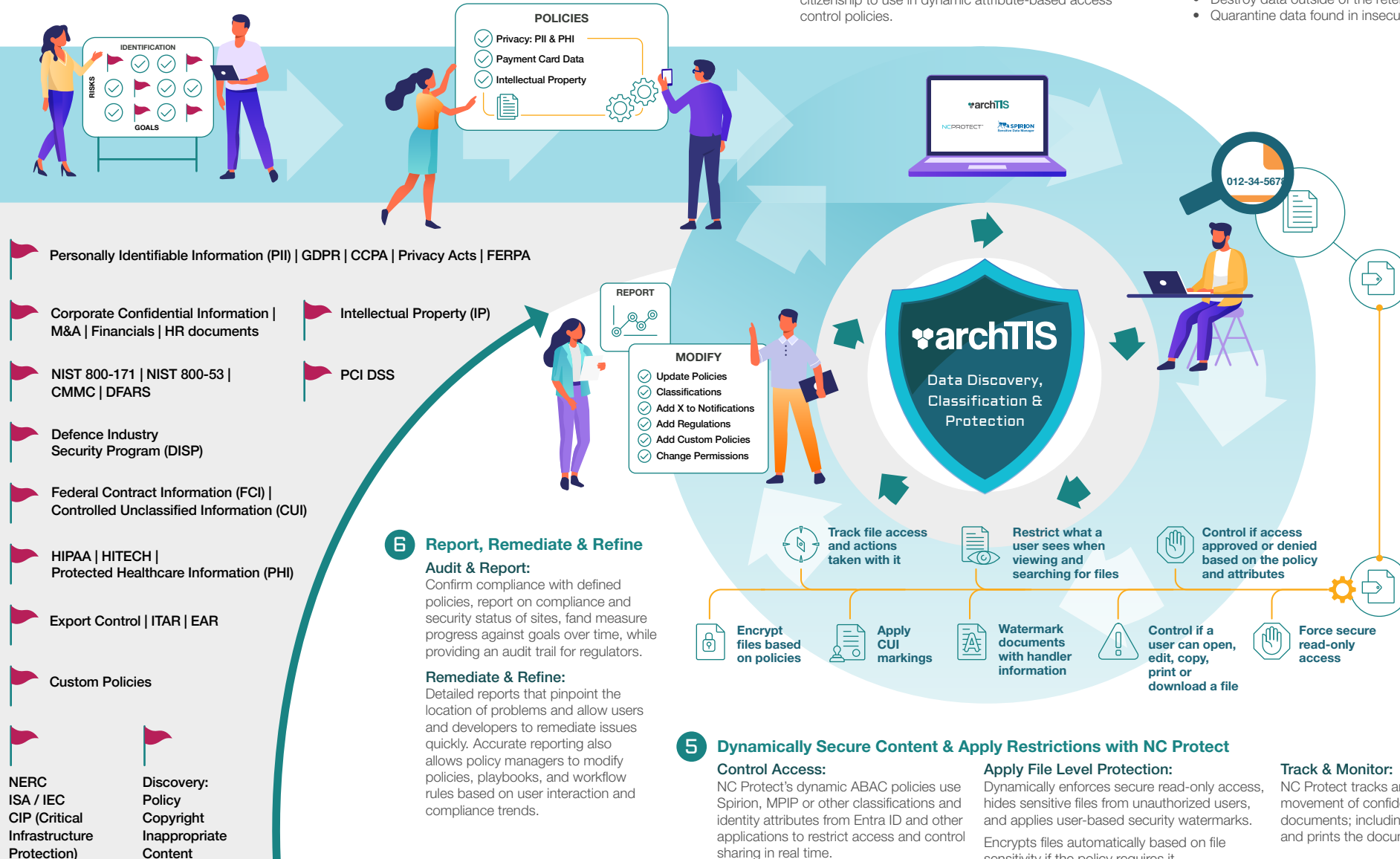
4 Discover & Classify Content with Spirion SDP

Scan:

Use Spirion SDP to scan and classify content based on the defined policy.

Remediate:

- Automatically classify confidential and sensitive documents with Spirion SDP context-rich classifications and/or MPIP sensitivity labels based on the presence of sensitive content.
- Destroy data outside of the retention policy.
- Quarantine data found in insecure locations.



Tips for Successful Data Security & Compliance

- Ensure your information security and compliance strategy aligns with the organization's overall strategy.
- Change your security approach - instead of defining groups, refine user attributes and claims.
- Have key stakeholders review the strategy regularly for changes, new policies and laws.
- Implement a solution to continuously audit content and user actions, detect violations and enforce policies to maintain data integrity, security and compliance.

Protect Your Data with Dynamic, Content and Context Aware Security

- Discover Sensitive Data**
Scan content to locate sensitive data.
- Classify Data**
Classify data at the file level based on pre-defined policies or users can manually classify data using pre-defined values.
- Restrict Access**
Set access control and file protection based on labels/classifications in combination with user attributes to dynamically control access, hide files, enforce read only access, apply watermarks, etc.
- Encrypt**
Further secure sensitive content by encrypting it immediately so only authorized users will be able to read the content—whether inside or outside of SharePoint or Microsoft 365.
- Control Distribution & Sharing**
Prevent users from sharing, copying, printing or downloading sensitive documents.
- Track & Audit**
Track and monitor the access, usage and sharing of confidential and sensitive documents; including who views, prints, and emails the documents. Export logs to Microsoft Sentinel for further actions and analysis.

archTIS
www.archTIS.com

Member of
Microsoft Intelligent
Security Association
Microsoft Security

Microsoft
Partner