

The below table maps NIST Privacy Controls with iDPS product features to help you adhere to NIST Privacy Framework.

CIS Control	CIS sub-control	Asset Type	Security Function	Title	Description	NIST 800-53 Controls	iDPS Features
3	3.1	Data	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	PR.IP-6	<p>Complete Data Governance/ Information Risk Solution</p> <p>Complete Data Scanning and Reporting with iDPS</p> <p>Provide visibility of permission on structured and unstructured Data</p>
3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	ID.AM-5	
3	3.6	Data	Identify	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.		
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	ID.AM-5	
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	ID.RA-5	
3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	PR.AC-4	