NIST Privacy Framework Core Changes: Preliminary Draft to Version 1.0

This document provides the changes between the NIST Privacy Framework Core in Version 1.0 from the Core published in the Preliminary Draft. Most significantly, two Subcategories were added to the Control Function under the Data Processing Management Category—CT.DM-P9 and CT.DM-P10—and one Subcategory was removed under the Disassociated Processing Category—CT-DP-P6. Minor changes detailed below were made to some Subcategories. These changes were primarily made to respond to stakeholder feedback and to clarify with examples and language adjustments to help facilitate better understanding.

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
IDENTIFY-P	Inventory and Mapping (ID.IM-P): Data processing by systems, products, or services is understood and informs the management of privacy risk. **No changes at the Category level.**	ID.IM-P1: Systems/products/services that process data are inventoried.	ID.IM-P1: Systems/products/services that process data are inventoried.	No Change
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	No Change
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	No Change
		ID.IM-P4: Data actions of the systems/products/services are inventoried.	ID.IM-P4: Data actions of the systems/products/services are inventoried.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
		ID.IM-P5: The purposes for the data actions are inventoried.	ID.IM-P5: The purposes for the data actions are inventoried.	No Change
		ID.IM-P6: Data elements within the data actions are inventoried.	ID.IM-P6: Data elements within the data actions are inventoried.	No Change
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	No Change
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	No Change
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used	ID.BE-P1: The organization's role**(s)** in the data processing ecosystem **are** identified and communicated.	ID.BE-P1: The organization's role in the data processing ecosystem is identified and communicated.	**Made "role" plural and corresponding grammar update to reflect that a single organization can have multiple roles in the data processing ecosystem environment.**
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	to inform privacy roles, responsibilities, and risk management decisions. **No changes at the Category level.**	ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	No Change
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity **and/or types**, visibility of data processing to individuals and third parties).	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity, visibility of data processing to individuals and third parties).	**Added "and/or types" to "data sensitivity" in examples of contextual factors.**
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	No Change
		ID.RA-P3: Potential problematic data actions and associated problems are identified.	ID.RA-P3: Potential problematic data actions and associated problems are identified.	No Change
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	No changes at the Category level.	ID.RA-P5: Risk responses are identified, prioritized, and implemented.	ID.RA-P5: Risk responses are identified, prioritized, and implemented.	No Change
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	ID.DE-P1: Data processing ecosystem risk management **policies**, processes, and **procedures** are identified, established, assessed, managed, and agreed to by organizational stakeholders.	ID.DE-P1: Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**Added "policies" and "procedures".**
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	No Change
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	No Change
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	No changes at the Category level.	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, **interoperability framework**, or other obligations.	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.	**Clarified scope of assessments to cover "interoperability framework" or "other" obligations.**
GOVERN-P	Governance Policies, Processes, and Procedures (GV.PO-P): The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. **Changed Category identifier from GV.PP to GV.PO.**	GV.**PO**-P1: Organizational privacy values and policies (e.g., conditions on data processing **such as data uses or retention periods**, individuals' prerogatives with respect to data processing) are established and communicated.	GV.PP-P1: Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	**Added examples of conditions on data processing: "data uses or retention periods". Changed Category identifier from GV.PP to GV.PO.**
		GV.**PO**-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	**Changed Category identifier from GV.PP to GV.PO.**
		GV.**PO**-P3: Roles and responsibilities for the workforce are established with respect to privacy.	GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.	**Changed Category identifier from GV.PP to GV.PO.**
		GV.**PO**-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	GV.PP-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	**Changed Category identifier from GV.PP to GV.PO.**

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
		GV.**PO**-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	**Changed Category identifier from GV.PP to GV.PO.**
		GV.**PO**-P6: Governance and risk management policies, processes, and procedures address privacy risks.	GV.PP-P6: Governance and risk management policies, processes, and procedures address privacy risks.	**Changed Category identifier from GV.PP to GV.PO.**
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. **No changes at the Category level.**	GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	No Change
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	No Change
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	GV.RM-P3: The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.	No Change
	Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy	GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.	GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.	No Change
		GV.AT-P2: Senior executives understand their roles and responsibilities.	GV.AT-P2: Senior executives understand their roles and responsibilities.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values. **No changes at the Category level.**	GV.AT-P3: Privacy personnel understand their roles and responsibilities.	GV.AT-P3: Privacy personnel understand their roles and responsibilities.	No Change
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	No Change
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment **(e.g., introduction of new technologies**), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	**Added an example of the introduction of new technologies as a key factor.**
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	No changes at the Category level.	GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	No Change
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	No Change
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, **professional events**).	GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers).	**Added "professional events" as a source of information on disclosure of problematic data actions.**
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	No Change
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.	GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
CONTROL-P	Data Processing Policies, Processes, and Procedures (CT.PO-P): Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy. **No changes at the Category level.**	CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	No Change
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place **(e.g., to maintain data quality, manage data retention)**.	CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place.	**Added examples of types of policies, processes, and procedures for enabling data review: "maintain data quality" and "manage data retention".**
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place	No Change
		CT.PO-P4: A **data** life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	**Changed "information" to "data".**
	Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect	CT.DM-P1: Data elements can be accessed for review.	CT.DM-P1: Data elements can be accessed for review.	No Change
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	CT.DM-P2: Data elements can be accessed for transmission or disclosure.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). **No changes at the Category level.**	CT.DM-P3: Data elements can be accessed for alteration.	CT.DM-P3: Data elements can be accessed for alteration.	No Change
		CT.DM-P4: Data elements can be accessed for deletion.	CT.DM-P4: Data elements can be accessed for deletion.	No Change
		CT.DM-P5: Data are destroyed according to policy.	CT.DM-P5: Data are destroyed according to policy.	No Change
		CT.DM-P6: Data are transmitted using standardized formats.	CT.DM-P6: Data are transmitted using standardized formats.	No Change
		CT.DM-P7: **Mechanisms for transmitting** processing permissions and related data values with data elements are established and in place.	CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.	**Changed "metadata…are transmitted" to "mechanisms for transmitting…are established and in place".**
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	No Change
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.	N/A	**This is a new Subcategory.**

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.	N/A	**This is a new Subcategory.**
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy **and enable implementation of privacy principles (e.g., data minimization)**. **Added "and enable implementation of privacy principles (e.g., data minimization)".**	CT.DP-P1: Data are processed **to limit observability and linkability** (e.g., data actions take place on local devices, privacy-preserving cryptography).	CT.DP-P1: Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography).	**Adjusted phrasing to "limit observability and linkability".**
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., **de-identification privacy techniques,** tokenization).	CT.DP-P2: Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	**Changed "differential privacy techniques" to "de-identification privacy techniques".**
		CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	No Change
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	No Change
		CT.DP-P5: Attribute references are substituted for attribute values.	CT.DP-P5: Attribute references are substituted for attribute values.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
		N/A	CT.DP-P6: Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives	**CT.DP-P6 was removed, and the principle of data minimization was added to the Category statement.**
COMMUNICATE-P	Communication Policies, Processes, and Procedures (CM.**PO**-P): Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks. **Changed Category identifier from CM.PP to CM.PO.**	CM.**PO**-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	CM.PP-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	**Changed Category identifier from CM.PP to CM.PO.**
		CM.**PO**-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	**Changed Category identifier from CM.PP to CM.PO.**

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy. **No changes at the Category level.**	CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	No Change
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.	CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.	No Change
		CM.AW-P3: System/product/service design enables data processing visibility.	CM.AW-P3: System/product/service design enables data processing visibility.	No Change
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	No Change
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure	No Change
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	No Change
		CM.AW-P8: Individuals are provided with mitigation mechanisms **(e.g., credit monitoring, consent withdrawal, data alteration or deletion)** to address impacts of problematic data actions.	CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.	**Added examples of mitigation mechanisms.**
PROTECT-P	Data Protection Policies, Processes, and Procedures (PR.**PO**-P): Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are	PR.**PO**-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	PR.DP-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P2: Configuration change control processes are established and in place.	PR.DP-P2: Configuration change control processes are established and in place.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P3: Backups of information are conducted, maintained, and tested.	PR.DP-P3: Backups of information are conducted, maintained, and tested.	**Changed Category identifier from PR.DP to PR.PO.**

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	maintained and used to manage the protection of data. **Changed Category identifier from PR.DP to PR.PO. Moved Category to be first listed in Function.**	PR.**PO**-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P5: Protection processes are improved.	PR.DP-P5: Protection processes are improved.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P6: Effectiveness of protection technologies is shared.	PR.DP-P6: Effectiveness of protection technologies is shared.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P8: Response and recovery plans are tested.	PR.DP-P8: Response and recovery plans are tested.	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	**Changed Category identifier from PR.DP to PR.PO.**
		PR.**PO**-P10: A vulnerability management plan is developed and implemented.	PR.DP-P10: A vulnerability management plan is developed and implemented.	**Changed Category identifier from PR.DP to PR.PO.**

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. **No changes at the Category level.**	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	No Change
		PR.AC-P2: Physical access to data and devices is managed.	PR.AC-P2: Physical access to data and devices is managed.	No Change
		PR.AC-P3: Remote access is managed.	PR.AC-P3: Remote access is managed.	No Change
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	No Change
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	No Change
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	No Change
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk	PR.DS-P1: Data-at-rest are protected.	PR.DS-P1: Data-at-rest are protected.	No Change
		PR.DS-P2: Data-in-transit are protected.	PR.DS-P2: Data-in-transit are protected.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability. **No changes at the Category level.**	PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	No Change
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	PR.DS-P4: Adequate capacity to ensure availability is maintained.	No Change
		PR.DS-P5: Protections against data leaks are implemented.	PR.DS-P5: Protections against data leaks are implemented.	No Change
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	No Change
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.	PR.DS-P7: The development and testing environment(s) are separate from the production environment.	No Change
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	No Change
	Maintenance (PR.MA-P): System maintenance and repairs are performed	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	No Change

	V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
	consistent with policies, processes, and procedures. **No changes at the Category level.**	PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	No Change
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements. **No changes at the Category level.**	PR.PT-P1: Removable media is protected and its use restricted according to policy.	PR.PT-P1: Removable media is protected and its use restricted according to policy.	No Change
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	No Change
		PR.PT-P3: Communications and control networks are protected.	PR.PT-P3: Communications and control networks are protected.	No Change
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	No Change