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
٩	Inventory and	ID.IM-P1: Systems/products/services	ID.IM-P1: Systems/products/services	No Change
DENTIFY-P	Mapping (ID.IM-P):	that process data are inventoried.	that process data are inventoried.	
Ξ	Data processing by			
	systems, products,	ID.IM-P2: Owners or operators (e.g.,	ID.IM-P2: Owners or operators (e.g.,	No Change
	or services is	the organization or third parties such	the organization or third parties such	
	understood and	as service providers, partners,	as service providers, partners,	
	informs the	customers, and developers) and their	customers, and developers) and their	
	management of	roles with respect to the	roles with respect to the	
	privacy risk.	systems/products/services and	systems/products/services and	
		components (e.g., internal or	components (e.g., internal or	
	No changes at the	external) that process data are	external) that process data are	
	Category level.	inventoried.	inventoried.	
		12.11.22.23.1		
		ID.IM-P3: Categories of individuals	ID.IM-P3: Categories of individuals	No Change
		(e.g., customers, employees or	(e.g., customers, employees or	
		prospective employees, consumers)	prospective employees, consumers)	
		whose data are being processed are	whose data are being processed are	
		inventoried.	inventoried.	
		ID.IM-P4: Data actions of the	ID.IM-P4: Data actions of the	No Change
		systems/products/services are	systems/products/services are	
		inventoried.	inventoried.	

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	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.
activities are understood and prioritized; this information is used	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	ID.BE-P3: Systems/products/services	ID.BE-P3: Systems/products/services	No Change
roles,	that support organizational priorities	that support organizational priorities	
responsibilities,	are identified and key requirements	are identified and key requirements	
and risk	communicated.	communicated.	
management			
decisions.			
No changes at the			
Category level.			
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	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-P2: Data analytic inputs and	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). ID.RA-P2: Data analytic inputs and	Added "and/or types" to "data sensitivity" in examples of contextual factors. No Change
operations, including mission, functions, other	outputs are identified and evaluated for bias.	outputs are identified and evaluated for bias.	NO Change
risk management priorities (e.g., compliance, financial),	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
reputation, workforce, and culture.	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
1	No changes at the	ID.RA-P5: Risk responses are	ID.RA-P5: Risk responses are	No Change
(Category level.	identified, prioritized, and	identified, prioritized, and	
		implemented.	implemented.	
	Data Processing	ID.DE-P1: Data processing ecosystem	ID.DE-P1: Data processing ecosystem	Added "policies" and
	Ecosystem Risk	risk management policies , processes,	risk management processes are	"procedures".
	Management	and procedures are identified,	identified, established, assessed,	
	(ID.DE-P): The	established, assessed, managed, and	managed, and agreed to by	
	organization's	agreed to by organizational	organizational stakeholders.	
	priorities,	stakeholders.		
	constraints, risk			
	tolerance, and	ID.DE-P2: Data processing ecosystem	ID.DE-P2: Data processing ecosystem	No Change
	assumptions are	parties (e.g., service providers,	parties (e.g., service providers,	
	established and	customers, partners, product	customers, partners, product	
	used to support	manufacturers, application	manufacturers, application	
	risk decisions	developers) are identified,	developers) are identified,	
	associated with	prioritized, and assessed using a	prioritized, and assessed using a	
	managing privacy	privacy risk assessment process.	privacy risk assessment process.	
1	risk and third			
	parties within the	ID.DE-P3: Contracts with data	ID.DE-P3: Contracts with data	No Change
	data processing	processing ecosystem parties are	processing ecosystem parties are	
	ecosystem. The	used to implement appropriate	used to implement appropriate	
	organization has	measures designed to meet the	measures designed to meet the	
	established and	objectives of an organization's	objectives of an organization's	
	implemented the	privacy program.	privacy program.	
	processes to			
	identify, assess,	ID.DE-P4: Interoperability	ID.DE-P4: Interoperability	No Change
	and manage	frameworks or similar multi-party	frameworks or similar multi-party	
	privacy risks within	approaches are used to manage data	approaches are used to manage data	
	the data processing	processing ecosystem privacy risks.	processing ecosystem privacy risks.	
	ecosystem.			

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

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

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

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

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

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	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".
organization's risk strategy to protect individuals' privacy and enable implementation of	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".
privacy principles (e.g., data minimization). Added "and enable implementation of privacy principles	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
(e.g., data minimization)".	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	CT.DP-P6 was removed, and the
			to that which is relevant and	principle of data minimization
			necessary for a system/product/service to meet	was added to the Category statement.
			mission/business objectives	statement.
			mission, susmess objectives	
<u>م</u>	Communication	CM. PO -P1: Transparency policies,	CM.PP-P1: Transparency policies,	Changed Category identifier
Ė	Policies, Processes,	processes, and procedures for	processes, and procedures for	from CM.PP to CM.PO.
2	and Procedures	communicating data processing	communicating data processing	
Ę	(CM. PO -P):	purposes, practices, and associated	purposes, practices, and associated	
COMMUNICATE-P	Policies, processes,	privacy risks are established and in	privacy risks are established and in	
8	and procedures are maintained and	place.	place.	
	used to increase	CM. PO -P2: Roles and responsibilities	CM.PP-P2: Roles and responsibilities	Changed Category identifier
	transparency of the	(e.g., public relations) for	(e.g., public relations) for	from CM.PP to CM.PO.
	organization's data	communicating data processing	communicating data processing	
	processing	purposes, practices, and associated	purposes, practices, and associated	
	practices (e.g.,	privacy risks are established.	privacy risks are established.	
	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.			

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

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

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

V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
Identity	PR.AC-P1: Identities and credentials	PR.AC-P1: Identities and credentials	No Change
Management,	are issued, managed, verified,	are issued, managed, verified,	
Authentication,	revoked, and audited for authorized	revoked, and audited for authorized	
and Access Control	individuals, processes, and devices.	individuals, processes, and devices.	
(PR.AC-P): Access			
to data and devices	PR.AC-P2: Physical access to data and	PR.AC-P2: Physical access to data and	No Change
is limited to	devices is managed.	devices is managed.	
authorized			
individuals,	PR.AC-P3: Remote access is	PR.AC-P3: Remote access is	No Change
processes, and	managed.	managed.	
devices, and is			21
managed consistent with the	PR.AC-P4: Access permissions and	PR.AC-P4: Access permissions and	No Change
assessed risk of	authorizations are managed,	authorizations are managed,	
unauthorized	incorporating the principles of least privilege and separation of duties.	incorporating the principles of least privilege and separation of duties.	
access.	privilege and separation of duties.	privilege and separation of duties.	
decess.	PR.AC-P5: Network integrity is	PR.AC-P5: Network integrity is	No Change
No changes at the	protected (e.g., network segregation,	protected (e.g., network segregation,	No change
Category level.	network segmentation).	network segmentation).	
0 ,	network segmentation).	network segmentation,	
	PR.AC-P6: Individuals and devices are	PR.AC-P6: Individuals and devices are	No Change
	proofed and bound to credentials,	proofed and bound to credentials,	
	and authenticated commensurate	and authenticated commensurate	
	with the risk of the transaction (e.g.,	with the risk of the transaction (e.g.,	
	individuals' security and privacy risks	individuals' security and privacy risks	
	and other organizational risks).	and other organizational risks).	
Data Security	PR.DS-P1: Data-at-rest are protected.	PR.DS-P1: Data-at-rest are protected.	No Change
(PR.DS-P): Data are			
managed	PR.DS-P2: Data-in-transit are	PR.DS-P2: Data-in-transit are	No Change
consistent with the	protected.	protected.	
organization's risk			

V1.0 CATEGORY	V1.0 SUBCATEGORY	PRELIMINARY DRAFT SUBCATEGORY	DESCRIPTION OF CHANGE
strategy to protect	PR.DS-P3: Systems/products/services	PR.DS-P3: Systems/products/services	No Change
individuals' privacy	and associated data are formally	and associated data are formally	
and maintain data	managed throughout removal,	managed throughout removal,	
confidentiality,	transfers, and disposition.	transfers, and disposition.	
integrity, and			
availability.	PR.DS-P4: Adequate capacity to	PR.DS-P4: Adequate capacity to	No Change
	ensure availability is maintained.	ensure availability is maintained.	
No changes at the			
Category level.	PR.DS-P5: Protections against data	PR.DS-P5: Protections against data	No Change
	leaks are implemented.	leaks are implemented.	
	PR.DS-P6: Integrity checking	PR.DS-P6: Integrity checking	No Change
	mechanisms are used to verify	mechanisms are used to verify	
	software, firmware, and information	software, firmware, and information	
	integrity.	integrity.	
	PR.DS-P7: The development and	PR.DS-P7: The development and	No Change
	testing environment(s) are separate	testing environment(s) are separate	
	from the production environment.	from the production environment.	
	PR.DS-P8: Integrity checking	PR.DS-P8: Integrity checking	No Change
	mechanisms are used to verify	mechanisms are used to verify	
	hardware integrity.	hardware integrity.	
Maintenance	PR.MA-P1: Maintenance and repair	PR.MA-P1: Maintenance and repair	No Change
(PR.MA-P): System	of organizational assets are	of organizational assets are	
maintenance and	performed and logged, with	performed and logged, with	
repairs are	approved and controlled tools.	approved and controlled tools.	
performed	1		

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