

YOUR LOGO GOES HERE

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

CMMC Level 1 / FAR 52.204-21

ACME Professional Services, LLP

SENSITIVE

Access Limited to Authorized Personnel

TABLE OF CONTENTS

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP) OVERVIEW	5
MANAGEMENT COMMITMENT	5
PURPOSE	5
SCOPE & APPLICABILITY	6
PEOPLE, PROCESSES, TECHNOLOGY, DATA & FACILITIES (PPTDF) CONTROL APPLICABILITY	6
ROLES	7
RESPONSIBILITIES	7
VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES	7
EXCEPTION TO STANDARDS	7
UPDATES TO POLICIES & STANDARDS	7
KEY TERMINOLOGY	8
CYBERSECURITY & DATA PROTECTION PROGRAM STRUCTURE	12
MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION	12
POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	12
CYBERSECURITY & DATA PROTECTION (GOV) POLICY & STANDARDS	13
GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM	13
GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION	13
GOV-04: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES	14
GOV-15: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES	14
ASSET MANAGEMENT (AST) POLICY & STANDARDS	15
AST-01: ASSET GOVERNANCE	15
AST-02: ASSET INVENTORIES	15
AST-02.8: ASSET INVENTORIES DATA ACTION MAPPING	16
AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	16
AST-09: SECURE DISPOSAL, DESTRUCTION OR RE-USE OF EQUIPMENT	17
AST-16: BRING YOUR OWN DEVICE (BYOD) USAGE	18
AST-17: PROHIBITED EQUIPMENT & SERVICES	18
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) POLICY & STANDARDS	20
BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	20
BCD-04: CONTINGENCY PLAN TESTING & EXERCISES	20
BCD-11: DATA BACKUPS	21
CHANGE MANAGEMENT (CHG) POLICY & STANDARDS	24
CHG-01: CHANGE MANAGEMENT PROGRAM	24
CHG-02: CONFIGURATION CHANGE CONTROL	25
CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES	25
CLOUD SECURITY (CLD) POLICY & STANDARDS	27
CLD-01: CLOUD SERVICES	27
CLD-02: CLOUD SECURITY ARCHITECTURE	27
CLD-06: MULTI-TENANT ENVIRONMENTS	28
CLD-10: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS	28
COMPLIANCE (CPL) POLICY & STANDARDS	29
CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	29
CONFIGURATION MANAGEMENT (CFG) POLICY & STANDARDS	30
CFG-01: CONFIGURATION MANAGEMENT PROGRAM	30
CFG-02: SECURE BASELINE CONFIGURATIONS	30
CFG-03: LEAST FUNCTIONALITY	32
CONTINUOUS MONITORING (MON) POLICY & STANDARDS	34
MON-01: CONTINUOUS MONITORING	34
MON-01.8: CONTINUOUS MONITORING SECURITY EVENT MONITORING	35
MON-03: CONTENT OF EVENT LOGS	36
MON-16: ANOMALOUS BEHAVIOR	37
CRYPTOGRAPHIC PROTECTIONS (CRY) POLICY & STANDARDS	38
CRY-01: USE OF CRYPTOGRAPHIC CONTROLS	38
CRY-03: TRANSMISSION CONFIDENTIALITY	39

CRY-05: ENCRYPTING DATA AT REST	40
CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT	40
DATA CLASSIFICATION & HANDLING (DCH) POLICY & STANDARDS	43
DCH-01: DATA PROTECTION	43
<i>DCH-01.2: DATA PROTECTION SENSITIVE/REGULATED DATA PROTECTION</i>	43
<i>DCH-01.4: DATA PROTECTION DEFINING ACCESS AUTHORIZATIONS FOR SENSITIVE / REGULATED DATA</i>	44
DCH-02: DATA & ASSET CLASSIFICATION	44
DCH-08: PHYSICAL MEDIA DISPOSAL	45
DCH-09: SYSTEM MEDIA SANITIZATION	45
DCH-13: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	46
<i>DCH-13.1: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) LIMITS OF AUTHORIZED USE</i>	47
DCH-15: PUBLICLY ACCESSIBLE CONTENT	47
DCH-17: AD-HOC TRANSFERS	48
ENDPOINT SECURITY (END) POLICY & STANDARDS	49
END-01: ENDPOINT DEVICE MANAGEMENT (EDM)	49
END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	49
<i>END-04.1: MALICIOUS CODE PROTECTION (ANTI-MALWARE) AUTOMATIC ANTIMALWARE SIGNATURE UPDATES</i>	50
<i>END-04.7: MALICIOUS CODE PROTECTION (ANTI-MALWARE) ALWAYS ON PROTECTION</i>	50
END-08: PHISHING & SPAM PROTECTION	51
HUMAN RESOURCES SECURITY (HRS) POLICY & STANDARDS	52
HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	52
HRS-04: PERSONNEL SCREENING	52
<i>HRS-04.1: PERSONNEL SCREENING ROLES WITH SPECIAL PROTECTION MEASURES</i>	53
HRS-05: TERMS OF EMPLOYMENT	53
<i>HRS-05.1: TERMS OF EMPLOYMENT RULES OF BEHAVIOR</i>	53
<i>HRS-05.2: TERMS OF EMPLOYMENT SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS</i>	54
IDENTIFICATION & AUTHENTICATION (IAC) POLICY & STANDARDS	56
IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	56
<i>IAC-01.3: IDENTITY & ACCESS MANAGEMENT (IAM) USER & SERVICE ACCOUNT INVENTORIES</i>	57
IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	57
IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	57
IAC-06: MULTI-FACTOR AUTHENTICATION (MFA)	58
IAC-07: USER PROVISIONING & DE-PROVISIONING	58
IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	59
IAC-10: AUTHENTICATOR MANAGEMENT	60
<i>IAC-10.8: AUTHENTICATOR MANAGEMENT DEFAULT AUTHENTICATORS</i>	61
IAC-15: ACCOUNT MANAGEMENT	62
<i>IAC-15.1: ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT (DIRECTORY SERVICES)</i>	64
IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)	64
IAC-17: PERIODIC REVIEW OF ACCOUNT PRIVILEGES	65
IAC-20: ACCESS ENFORCEMENT	66
IAC-21: LEAST PRIVILEGE	66
INCIDENT RESPONSE (IRO) POLICY & STANDARDS	68
IRO-01: INCIDENTS RESPONSE OPERATIONS	68
IRO-02: INCIDENT HANDLING	68
IRO-04: INCIDENT RESPONSE PLAN (IRP)	69
NETWORK SECURITY (NET) POLICY & STANDARDS	71
NET-01: NETWORK SECURITY CONTROLS (NSC)	71
NET-02: LAYERED DEFENSES	71
<i>NET-02.2: LAYERED DEFENSES GUEST NETWORKS</i>	72
NET-03: BOUNDARY PROTECTION	72
NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)	73
NET-06: NETWORK SEGMENTATION (MACROSEGMENTATION)	74
NET-14: REMOTE ACCESS	74
<i>NET-14.5: REMOTE ACCESS WORK FROM ANYWHERE (WFA) – TELECOMMUTING SECURITY</i>	75
NET-15: WIRELESS NETWORKING	75

NET-18: DNS & CONTENT FILTERING	76
PHYSICAL & ENVIRONMENTAL SECURITY (PES) POLICY & STANDARDS	77
PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS	77
PES-02: PHYSICAL ACCESS AUTHORIZATIONS	77
<i>PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS ROLE-BASED PHYSICAL ACCESS</i>	78
PES-03: PHYSICAL ACCESS CONTROL	78
<i>PES-03.3: PHYSICAL ACCESS CONTROL PHYSICAL ACCESS LOGS</i>	79
<i>PES-03.4: PHYSICAL ACCESS CONTROL ACCESS TO INFORMATION SYSTEMS</i>	80
PES-06: VISITOR CONTROL	80
<i>PES-06.1: VISITOR CONTROL DISTINGUISH VISITORS FROM ON-SITE PERSONNEL</i>	81
<i>PES-06.3: VISITOR CONTROL RESTRICT UNESCORTED ACCESS</i>	81
PES-12: EQUIPMENT SITING & PROTECTION	81
<i>PES-12.1: EQUIPMENT SITING & PROTECTION TRANSMISSION MEDIUM SECURITY</i>	82
<i>PES-12.2: EQUIPMENT SITING & PROTECTION ACCESS CONTROL FOR OUTPUT DEVICES</i>	82
RISK MANAGEMENT (RSK) POLICY & STANDARDS	83
RSK-01: RISK MANAGEMENT PROGRAM (RMP)	83
RSK-03: RISK IDENTIFICATION	83
RSK-04: RISK ASSESSMENT	84
<i>RSK-04.1: RISK ASSESSMENT RISK REGISTER</i>	85
RSK-06: RISK REMEDIATION	85
SECURITY AWARENESS & TRAINING (SAT) POLICY & STANDARDS	86
SAT-01: CYBERSECURITY & DATA PROTECTION-MINDED WORKFORCE	86
SAT-02: CYBERSECURITY & DATA PROTECTION AWARENESS TRAINING	87
THIRD-PARTY MANAGEMENT (TPM) POLICY & STANDARDS	89
TPM-01: THIRD-PARTY MANAGEMENT	89
<i>TPM-01.1: THIRD-PARTY MANAGEMENT THIRD-PARTY INVENTORIES</i>	90
TPM-03: SUPPLY CHAIN RISK MANAGEMENT (SCRM)	90
TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	90
<i>TPM-05.2: THIRD-PARTY CONTRACT REQUIREMENTS CONTRACT FLOW-DOWN REQUIREMENTS</i>	91
<i>TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX</i>	92
TPM-08: REVIEW OF THIRD-PARTY SERVICES	92
VULNERABILITY & PATCH MANAGEMENT (VPM) POLICY & STANDARDS	94
VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	94
VPM-02: VULNERABILITY REMEDIATION PROCESS	94
VPM-05: SOFTWARE & FIRMWARE PATCHING	95
VPM-06: VULNERABILITY SCANNING	97
WEB SECURITY (WEB) POLICY & STANDARDS	100
WEB-01: WEB SECURITY	100
WEB-02: USE OF DEMILITARIZED ZONES (DMZs)	100
WEB-04: CLIENT-FACING WEB SERVICES	100
GLOSSARY: ACRONYMS & DEFINITIONS	102
ACRONYMS	102
DEFINITIONS	103
RECORD OF CHANGES	104

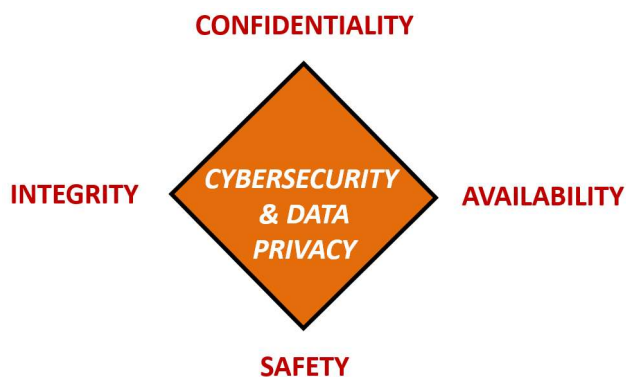
CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP) OVERVIEW

MANAGEMENT COMMITMENT

The **Cybersecurity & Data Protection Program (CDPP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Professional Services, LLP (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with ACME's Technology Assets, Applications, Services and/or Data (TAASD). Therefore, it is the responsibility of both ACME personnel and third-parties to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, cybersecurity and data protection measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of TAASD. This also includes protection against accidental loss or destruction. The security of Technology Assets, Applications and/or Services (TAAS) must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **CONFIDENTIALITY** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- **INTEGRITY** – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **AVAILABILITY** – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **SAFETY** – This addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

PURPOSE

The purpose of the Cybersecurity & Data Protection Program (CDPP) is to:

- Create a leading practice-based Information Security Management System (ISMS);
- Protect the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME data and systems;
- Protect ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensure the effectiveness of cybersecurity and data protection controls over data and systems that support ACME's operations; and
- Provide for the development, review and maintenance of the cybersecurity and data protection controls required to protect ACME's data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which ACME operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related control objectives, standards, procedures and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure ACME personnel understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of ACME data.

SCOPE & APPLICABILITY

These policies, standards and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards and guidelines apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME data.

PEOPLE, PROCESSES, TECHNOLOGY, DATA & FACILITIES (PPTDF) CONTROL APPLICABILITY

Control scoping does not mean all controls apply uniformly to every asset, individual or facility. This misunderstanding of applicability vs scoping is one of the biggest hurdles that organizations face, since there is a common misconception that if something is “in scope” then every control will be applicable across the entire boundary of the assessment. This is an incorrect assumption. When looking at the breath of controls that an organization is obligated to comply with, the controls are often administrative, technical or physical in nature. This means that there may be controls that are not applicable to certain systems, applications and/or processes.

Example 1: Network firewall

- A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- A network firewall is a device. Therefore, a network firewall is not capable of undergoing end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.

Example 2: User awareness training

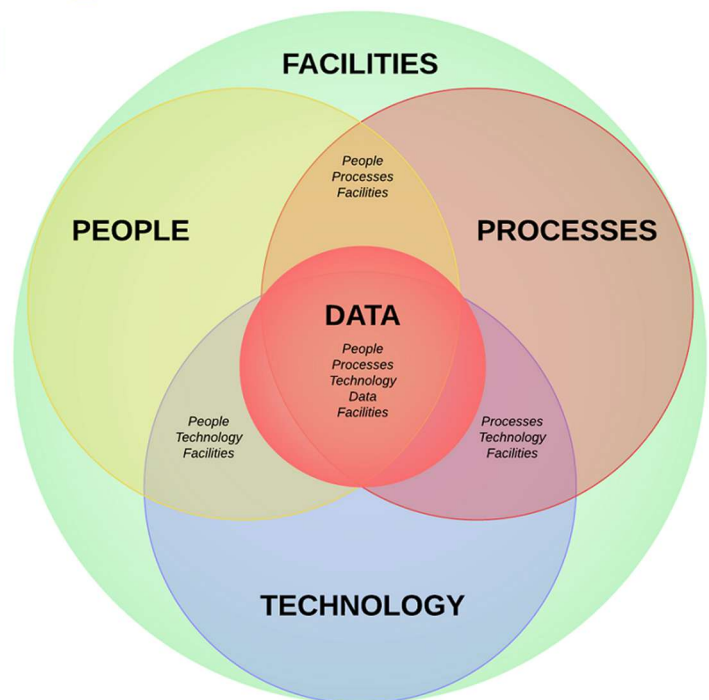
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.

Example 3: Incident Response Plan (IRP)

- An IRP is a documented process that guides incident response operations.
- An IRP is not an individual or technology. Therefore, an IRP cannot sign an NDA, have MFA or be patched.

The People, Processes, Technology, Data and Facilities (PPTDF) model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls.

- People. Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
- Processes. Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
- Technology. Control directly applies to Technology Assets, Applications and/or Services (TAAS) (e.g., secure baseline configurations, patching, etc.).
- Data. Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
- Facilities. Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



CYBERSECURITY & DATA PROTECTION (GOV) POLICY & STANDARDS

Management Intent: The purpose of the Cybersecurity & Data Protection (GOV) policy is to govern a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity and data protection principles that addresses all applicable statutory, regulatory and contractual obligations.

Policy: ACME shall tailor cybersecurity and data protection controls accordingly so that cost-effective controls can be applied commensurately with the risk and sensitivity of the data and technologies in use, ensuring applicable security, compliance and resilience requirements are sufficiently addressed.

ACME shall implement and maintain a maturity-based capability to strengthen the security and resilience of its technology infrastructure and data protection mechanisms against both physical and cyber threats. Security control decisions shall take applicable statutory, regulatory and contractual obligations into account, but ACME acknowledges that being compliant does not equate to being secure, so all stakeholders shall protect the confidentiality, integrity, availability and safety of ACME's technology resources and data, regardless of the geographic location of the data or technology in use.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

Control Objective: The organization facilitates the implementation of cybersecurity and data protection governance controls.¹⁰

Standard: ACME's cybersecurity and data protection policies and standards must be represented in a single document, the Cybersecurity & Data Protection Program (CDPP) that:

- (a) Must be reviewed and updated at least annually; and
- (b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

Guidelines: The security plans for individual systems and the organization-wide DSP together provide complete coverage for all cybersecurity and data protection-related controls employed within the organization.

GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

Control Objective: The organization establishes, maintains and disseminates cybersecurity and data protection policies, standards and procedures.¹¹

Standard: The Cybersecurity & Data Protection Program (CDPP) document represents the consolidation of ACME's cybersecurity and data protection policies and standards. The DSP is endorsed by ACME's executive management and shall be:

- (a) Disseminated to the appropriate parties to ensure all affected personnel are made aware of and understand their applicable requirements to protect cardholder data;
- (b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the DSP, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;
- (c) Enforced by ACME personnel through "business as usual" secure practices in the form of Standardized Operating Procedures (SOP) that shall be developed, enforced and maintained at the control operator level; and
- (d) Enforced through ACME's supply chain in the form of contractual requirements with those third-parties that have the ability to directly or indirectly influence the confidentiality, integrity and/or availability of ACME's Technology Assets, Applications and/or Services (TAAS) and/or sensitive/regulated data.

¹⁰ ISO 27001-2013: 4.3, 4.4, 5.1, 6.1.1 | ISO 27002-2022: 5.1, 5.4, 5.37 | NIST SP 800-53 R5: PM-1 | NIST SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV, GV.RM-01, GV.RM-03, GV.RR-01, GV.SC, GV.SC-01, GV.SC-03, GV.SC-09, ID.RA, PR, PR.IR

¹¹ ISO 27001-2013: 4.3, 5.2, 7.5.1, 7.5.2, 7.5.3 | ISO 27002-2022: 5.1, 5.37 | NIST SP 800-53 R5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1 | NIST SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV.PO, GV.PO-01, GV.SC-01, GV.SC-03, ID.RA

ASSET MANAGEMENT (AST) POLICY & STANDARDS

Management Intent: The purpose of the Asset Management (AST) policy is to ensure that Technology Assets, Applications and/or Services (TAAS) are properly managed throughout the lifecycle of the asset, from procurement through disposal.

Policy: ACME shall implement and maintain appropriate IT Asset Management (ITAM) practices to strengthen the security, compliance and resilience of its technology infrastructure and data protection capabilities against both physical and cyber threats.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

AST-01: ASSET GOVERNANCE

Control Objective: The organization facilitates an IT Asset Management (ITAM) program to implement and manage asset management controls.¹⁴

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that includes, but is not limited to:

- (a) Maintaining an accurate and current list of IT assets that includes but is not limited to:
 1. Make and model of the device;
 2. Location of device; and
 3. Device serial number or other methods of unique identification;
- (b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices); and
- (c) A list of company-approved products.

Guidelines: It is also possible that the owner and custodian of the hardware, software and data are the same, but this needs to be identified and documented.

AST-02: ASSET INVENTORIES

Control Objective: The organization performs inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:

- (1) Accurately reflects the current TAASD in use;
- (2) Identifies authorized software products, including business justification details;
- (3) Is at the level of granularity deemed necessary for tracking and reporting;
- (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and
- (5) Is available for review and audit by designated organizational personnel.

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that inventories ACME's Technology Assets, Applications, Services and/or Data (TAASD) as follows:

- (a) Hardware and software inventories, both:
 1. Internally-hosted Technology Assets, Applications and/or Services (TAAS); and
 2. Externally-hosted TAAS;
- (b) Sensitive/regulated data that is stored, processed and/or transmitted on the TAAS;
- (c) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices);
- (d) List of ACME-approved TAAS (e.g., software and hardware);
- (e) Review and update inventories at least quarterly; and
- (f) Where technically feasible, a list of all personnel with access to assets.

¹⁴ ISO 27001-2013: 4.2 | ISO 27002-2022: 5.30, 5.31, 7.9 | NIST SP 800-53 R5: PM-5 | NIST SP 800-171 R2: 3.4.1, 3.8.3 | NIST SP 800-171 R3: 03.01.03, 03.01.18.a, 03.04.11.a, 03.07.04.a | NIST CSF 2.0: GV.SC-04, ID.AM, ID.AM-08 | FAR 52.204-21(b)(1)(vii)