YOUR LOGO GOES HERE

NIST 800-171 R2 COMPLIANCE PROGRAM (NCP)

POLICIES & STANDARDS

ACME Consultants, LLP

EXAMPLE

SENSITIVE

Access Limited to Authorized Personnel

Table of Contents

Notice – Referenced Frameworks & Supporting Practices 9

NIST 800-171 Compliance Program (NCP) Overview 10

Management Commitment 10

Purpose 10

Scope & Applicability 11

People, Processes, Technology, Data, Facilities & Artificial Intelligence (PPTDF-AI) Control Applicability 11

Roles 12

Responsibilities 12

Violations of Policies, Standards and/or Procedures 12

Exception To Standards 12

Updates To Policies & Standards 12

Key Terminology 12

Security, Compliance and Resilience Program Structure 18

Management Direction for Security, Compliance and Resilience 18

Plan, Do, Check & Act (PDCA) Approach To Security, Compliance and Resilience 18

Policies, Controls, Standards, Procedures & Guidelines Structure 19

Security, Compliance and Resilience Governance (GOV) Policy & Standards 20

GOV-01: Security, Compliance and Resilience Program (NCP) 20

GOV-02: Publishing Security, Compliance and Resilience Documentation 20

GOV-04: Assigned Security, Compliance and Resilience Responsibilities 21

GOV-04.1: Assigned Security, Compliance and Resilience Responsibilities | Accountability Structure 21

GOV-15: Operationalizing Security, Compliance and Resilience Practices 21

GOV-15.1: Operationalizing Security, Compliance and Resilience Practices | Select Controls 22

GOV-15.2: Operationalizing Security, Compliance and Resilience Practices | Implement Controls 22

GOV-15.3: Operationalizing Security, Compliance and Resilience Practices | Assess Controls 23

GOV-15.4: Operationalizing Security, Compliance and Resilience Practices | Authorize Technology Assets, Applications and/or Services (TAAS) 23

GOV-15.5: Operationalizing Security, Compliance and Resilience Practices | Monitor Controls 23

GOV-17: Security, Compliance and Resilience Status Reporting 23

Asset Management (AST) Policy & Standards 25

AST-01: Asset Governance 25

AST-02: Asset Inventories 25

AST-02.1: Asset Inventories | Updates During Installations/Removals 26

AST-02.3: Asset Inventories | Component Duplication Avoidance 26

AST-05: Security of Assets & Media 26

AST-09: Secure Disposal, Destruction or Re-Use of Equipment 27

AST-16: Bring Your Own Device (BYOD) Usage 27

AST-17: Prohibited Equipment & Services 28

Business Continuity & Disaster Recovery (BCD) Policy & Standards 29

BCD-01: Business Continuity Management System (BCMS) 29

BCD-11: Data Backups 30

BCD-11.4: Data Backups | Cryptographic Protection 32

Change Management (CHG) Policy & Standards 33

CHG-01: Change Management Program 33

CHG-02: Configuration Change Control 34

CHG-02.2: Configuration Change Control | Test, Validate & Document Changes 34

CHG-03: Security Impact Analysis for Changes 35

CHG-04: Access Restriction For Change 35

CHG-05: Stakeholder Notification of Changes 35

Cloud Security (CLD) Policy & Standards 36

CLD-01: Cloud Services 36

CLD-02: Cloud Security Architecture 36

CLD-03: Cloud Infrastructure Security Subnet 37

CLD-06: Multi-Tenant Environments 37

EXAMPLE

CLD-10: Sensitive Data In Public Cloud Providers 37

Compliance (CPL) Policy & Standards 38

CPL-01: Statutory, Regulatory & Contractual Compliance 38

CPL-01.7: Statutory, Regulatory & Contractual Compliance | Designated Certifying Official 38

CPL-01.8: Statutory, Regulatory & Contractual Compliance | Conformity Attestations 38

CPL-02: Security, Compliance and Resilience Controls Oversight 39

CPL-02.1: Security, Compliance and Resilience Controls Oversight | Internal Audit Function 39

CPL-03: Security, Compliance and Resilience Assessments 40

CPL-03.1: Security, Compliance and Resilience Assessments | Independent Assessors 40

Configuration Management (CFG) Policy & Standards 41

CFG-01: Configuration Management Program 41

CFG-02: Secure Baseline Configurations 41

CFG-02.1: System Hardening Through Baseline Configurations | Reviews & Updates 43

CFG-02.5: Secure Baseline Configurations | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas 43

CFG-02.9: Secure Baseline Configurations | Baseline Tailoring 44

CFG-03: Least Functionality 45

CFG-03.1: Least Functionality | Periodic Review 46

CFG-03.2: Least Functionality | Prevent Unauthorized Software Execution 46

CFG-03.3: Least Functionality | Explicitly Allow / Deny Applications 47

CFG-03.4: Least Functionality | Split Tunneling 47

CFG-05: User-Installed Software 48

Continuous Monitoring (MON) Policy & Standards 49

MON-01: Continuous Monitoring 49

MON-01.3: Continuous Monitoring | Inbound & Outbound Communications Traffic 50

MON-01.4: Continuous Monitoring | System Generated Alerts 51

MON-01.8: Continuous Monitoring | Security Event Monitoring 52

MON-01.16: Continuous Monitoring | Analyze & Prioritize Monitoring Requirements 52

MON-02: Centralized Event Log Collection 53

MON-02.1: Centralized Event Log Collection | Correlate Monitoring Information 54

MON-03: Content of Event Logs 54

MON-03.1: Content Of Event Logs | Sensitive Event Log Information 55

MON-03.2: Content Of Event Logs | Audit Trails 56

MON-03.7: Content Of Event Logs | Database Logging 56

MON-05: Response To Event Log Processing Failures 56

MON-06: Monitoring Reporting 57

MON-07: Time Stamps 57

MON-07.1: Time Stamps | Synchronization With Authoritative Time Source 58

MON-08: Protection of Event Logs 58

MON-08.2: Protection of Event Logs | Access by Subset of Privileged Users 58

MON-10: Event Log Retention 59

MON-11: Monitoring For Information Disclosure 59

MON-11.3: Monitoring For Information Disclosure | Monitoring for Indicators of Compromise (IOC) 60

MON-16: Anomalous Behavior 60

Cryptographic Protections (CRY) Policy & Standards 61

CRY-01: Use of Cryptographic Controls 61

CRY-01.1: Use of Cryptographic Controls | Alternate Physical Protection 62

CRY-03: Transmission Confidentiality 62

CRY-04: Transmission Integrity 63

CRY-05: Encrypting Data At Rest 63

CRY-08: Public Key Infrastructure (PKI) 64

CRY-09: Cryptographic Key Management 64

Data Classification & Handling (DCH) Policy & Standards 67

DCH-01: Data Protection 67

DCH-01.2: Data Protection | Sensitive/Regulated Data Protection 67

DCH-03: Media Access 68

EXAMPLE

DCH-04: Media Marking 68
DCH-06: Media Storage 69
DCH-07: Media Transportation 70
DCH-08: Physical Medial Disposal 70
DCH-09: System Media Sanitization 71
DCH-10: Media Use 71
DCH-10.2: Media Use | Prohibit Use Without Owner 72
DCH-13: Use of External Technology Assets, Applications and/or Services (TAAS) 72
DCH-13.1: Use of External Technology Assets, Applications and/or Services (TAAS) | Limits of Authorized Use 73
DCH-13.2: Use of External Technology Assets, Applications and/or Services (TAAS) | Portable Storage Devices 73
DCH-15: Publicly Accessible Content 74
DCH-17: Ad-Hoc Transfers 74

Endpoint Security (END) Policy & Standards 75
END-01: Endpoint Device Management (EDM) 75
END-02: Endpoint Protection Measures 75
END-03: Prohibit Installation Without Privileged Status 76
END-03.2: Prohibit Installation Without Privileged Status | Governing Access Restriction for Change 76
END-04: Malicious Code Protection (Anti-Malware) 76
END-04.1: Malicious Code Protection (Anti-malware) | Automatic Antimalware Signature Updates 77
END-04.7: Malicious Code Protection (Anti-malware) | Always On Protection 77
END-10: Mobile Code 78
END-14: Collaborative Computing Devices 79

Human Resources Security (HRS) Policy & Standards 80
HRS-01: Human Resources Security Management 80
HRS-01.1: Human Resources Security Management | Onboarding, Transferring & Offboarding Personnel 80
HRS-04: Personnel Screening 81
HRS-04.1: Personnel Screening | Roles With Special Protection Measures 81
HRS-04.2: Personnel Screening | Formal Indoctrination 82
HRS-05: Terms of Employment 82
HRS-05.1: Terms of Employment | Rules of Behavior 82
HRS-05.2: Terms of Employment | Social Media & Social Networking Restrictions 83
HRS-06: Access Agreements 83
HRS-07: Personnel Sanctions 84
HRS-08: Personnel Transfer 85
HRS-09: Personnel Termination 85
HRS-10: Third-Party Personnel 86
HRS-11: Separation of Duties (SoD) 87

Identification & Authentication (IAC) Policy & Standards 88
IAC-01: Identity & Access Management (IAM) 88
IAC-02: Identification & Authentication for Organizational Users 89
IAC-02.2: Identification & Authentication for Organizational Users | Replay-Resistant Authentication 89
IAC-04: Identification & Authentication for Devices 89
IAC-06: Multi-Factor Authentication (MFA) 90
IAC-06.1: Multi-Factor Authentication (MFA) | Network Access to Privileged Accounts 90
IAC-06.2: Multi-Factor Authentication (MFA) | Network Access to Non-Privileged Accounts 90
IAC-06.3: Multi-Factor Authentication (MFA) | Local Access to Privileged Accounts 91
IAC-08: Role-Based Access Control (RBAC) 91
IAC-09: Identifier Management (User Names) 92
IAC-09.5: Identifier Management | Privileged Account Identifiers 92
IAC-10: Authenticator Management 93
IAC-10.1: Authenticator Management | Password-Based Authentication 93
IAC-10.5: Authenticator Management | Protection of Authenticators 95
IAC-11: Authenticator Feedback 96
IAC-15: Account Management 96
IAC-15.1: Account Management | Automated System Account Management (Directory Services) 98
IAC-15.3: Account Management | Disable Inactive Accounts 99
IAC-16: Privileged Account Management (PAM) 99

EXAMPLE

IAC-16.1: Privileged Account Management (PAM) | Privileged Account Inventories 99
IAC-20: Access Enforcement 100
IAC-21: Least Privilege 100
IAC-21.1: Least Privilege | Authorize Access to Security Functions 101
IAC-21.2: Least Privilege | Non-Privileged Access for Non-Security Functions 101
IAC-21.3: Least Privilege | Management Approval For Privileged Accounts 101
IAC-21.4: Least Privilege | Auditing Use of Privileged Functions 102
IAC-21.5: Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions 102
IAC-22: Account Lockout 102
IAC-24: Session Lock 102
IAC-24.1: Session Lock | Pattern-Hiding Displays 103
IAC-25: Session Termination 103
Incident Response (IRO) Policy & Standards 104
IRO-01: Incidents Response Operations 104
IRO-02: Incident Handling 104
IRO-03: Indicators of Compromise (IOC) 105
IRO-04: Incident Response Plan (IRP) 105
IRO-04.2: Incident Response Plan (IRP) | IRP Update 106
IRO-05: Incident Response Training 106
IRO-06: Incident Response Testing 107
IRO-08: Chain of Custody & Forensics 107
IRO-10: Incident Stakeholder Reporting 107
IRO-10.2: Incident Stakeholder Reporting | Cyber Incident Reporting for Sensitive / Regulated Data 108
IRO-11: Incident Reporting Assistance 109
IRO-11.2: Incident Reporting Assistance | Coordination With External Providers 109
IRO-12: Sensitive / Regulated Data Spill Response 109
IRO-12.1: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Responsible Personnel 109
IRO-12.2: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Training 110
IRO-12.3: Sensitive / Regulated Data Spill Response | Post-Sensitive / Regulated Data Spill Operations 110
IRO-12.4: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Exposure to Unauthorized Personnel 110
IRO-13: Root Cause Analysis (RCA) & Lessons Learned 110
Information Assurance (IAO) Policy & Standards 112
IAO-01: Information Assurance (IA) Operations 112
IAO-01.1: Information Assurance (IA) Operations | Assessment Boundaries 112
IAO-02: Assessments 112
IAO-02.1: Assessments | Independent Assessors 113
IAO-03: Applied Security, Compliance and Resilience Controls Documentation 113
IAO-03.1: Applied Security, Compliance and Resilience Controls Documentation | Plan/Coordinate with Other Organizational Entities 115
IAO-03.2: Applied Security, Compliance and Resilience Controls Documentation | Adequate Security for Sensitive / Regulated Data In Support of Contracts 115
IAO-05: Capabilities Deficiency Tracking 116
Maintenance (MNT) Policy & Standards 118
MNT-01: Maintenance Operations 118
MNT-02: Controlled Maintenance 118
MNT-04: Maintenance Tools 119
MNT-04.2: Maintenance Tools | Inspect Media 119
MNT-05: Remote Maintenance 119
MNT-05.2: Remote Maintenance | Remote Maintenance Notifications 120
MNT-05.4: Remote Maintenance | Remote Maintenance Disconnect Verification 120
MNT-06: Maintenance Personnel 120
MNT-06.1: Maintenance Personnel | Maintenance Personnel Without Appropriate Access 121
MNT-06.2: Maintenance Personnel | Non-System Related Maintenance 121
Mobile Device Management (MDM) Policy & Standards 122
MDM-01: Centralized Management Of Mobile Devices 122
MDM-02: Access Control For Mobile Devices 122

EXAMPLE

MDM-03: Full Device & Container-Based Encryption 123
MDM-06: Personally-Owned Mobile Devices 123
MDM-07: Organization-Owned Mobile Devices 124

Network Security (NET) Policy & Standards 125
NET-01: Network Security Controls (NSC) 125
NET-02: Layered Defenses 125
NET-02.2: Layered Defenses | Guest Networks 126
NET-03: Boundary Protection 126
NET-03.1: Boundary Protection | Limit Network Connections 127
NET-03.2: Boundary Protection | External Telecommunications Services 127
NET-04: Data Flow Enforcement – Access Control Lists (ACLs) 128
NET-04.1: Data Flow Enforcement | Deny Traffic by Default & Allow Traffic by Exception 129
NET-05: Interconnection Security Agreements (ISAs) 129
NET-05.2: Interconnection Security Agreements (ISAs) | Internal System Connections 130
NET-06: Network Segmentation (macrosegementation) 131
NET-07: Network Connection Termination 131
NET-08: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) 131
NET-09: Session Integrity 132
NET-10: Domain Name Service (DNS) Resolution 132
NET-10.1: Domain Name Service (DNS) Resolution | Architecture & Provisioning For Name/Address Resolution Service 132
NET-10.2: Domain Name Service (DNS) Resolution | Secure Name/Address Resolution Service (Recursive or Caching Resolver) 133
NET-13: Electronic Messaging 133
NET-14: Remote Access 134
NET-14.1: Remote Access | Automated Monitoring & Control 134
NET-14.2: Remote Access | Protection of Confidentiality/Integrity Using Encryption 134
NET-14.3: Remote Access | Managed Access Control Points 135
NET-14.4: Remote Access | Privileged Commands & Access 135
NET-14.5: Remote Access | Work From Anywhere (WFA) – Telecommuting Security 135
NET-15: Wireless Networking 135
NET-15.1: Wireless Access | Authentication & Encryption 136
NET-18: DNS & Content Filtering 137

Physical & Environmental Security (PES) Policy & Standards 138
PES-01: Physical & Environmental Protections 138
PES-02: Physical Access Authorizations 138
PES-02.1: Physical Access Authorizations | Role-Based Physical Access 139
PES-03: Physical Access Control 139
PES-03.3: Physical Access Control | Physical Access Logs 140
PES-03.4: Physical Access Control | Access To Information Systems 141
PES-04: Physical Security of Offices, Rooms & Facilities 141
PES-05: Monitoring Physical Access 142
PES-05.1: Monitoring Physical Access | Intrusion Alarms/Surveillance Equipment 142
PES-05.2: Monitoring Physical Access | Monitoring Physical Access to Information Systems 143
PES-06: Visitor Control 143
PES-06.1: Visitor Control | Distinguish Visitors from On-Site Personnel 144
PES-06.3: Visitor Control | Restrict Unescorted Access 144
PES-10: Delivery & Removal 144
PES-11: Alternate Work Site 144
PES-12: Equipment Siting & Protection 145
PES-12.1: Equipment Siting & Protection | Transmission Medium Security 145
PES-12.2: Equipment Siting & Protection | Access Control For Output Devices 146

Project & Resource Management (PRM) Policy & Standards 147
PRM-01: Security, Compliance and Resilience Portfolio Management 147
PRM-03: Allocation of Resources 147
PRM-07: System Development Life Cycle (SDLC) Management 148

Risk Management (RSK) Policy & Standards 149

EXAMPLE

RSK-01: Risk Management Program (RMP) 149
RSK-04: Risk Assessment 150
RSK-06: Risk Remediation 151
RSK-06.2: Risk Remediation | Compensating Countermeasures 151
Secure Engineering & Architecture (SEA) Policy & Standards 152
SEA-01: Secure Engineering Principles 152
SEA-02: Alignment With Enterprise Architecture 153
SEA-02.1: Alignment With Enterprise Architecture | Standardized Terminology 154
SEA-03: Defense-In-Depth (DiD) Architecture 154
SEA-03.2: Defense-In-Depth (DiD) Architecture | Application Partitioning 155
SEA-04: Process Isolation 155
SEA-05: Information In Shared Resources 155
SEA-07: Predictable Failure Analysis 156
SEA-07.1: Predictable Failure Analysis | Technology Lifecycle Management 156
SEA-10: Memory Protection 157
SEA-18: System Use Notification (Logon Banner) 157
SEA-18.1: System Use Notification | Standardized Microsoft Windows Banner 157
SEA-18.2: System Use Notification | Truncated Banner 158
SEA-20: Clock Synchronization 158
Security Awareness & Training (SAT) Policy & Standards 159
SAT-01: Security, Compliance and Resilience-Minded Workforce 159
SAT-02: Security, Compliance and Resilience Awareness Training 160
SAT-03: Role-Based Security, Compliance & Resilience Training 161
SAT-03.6: Role-Based Security, Compliance & Resilience Training | Cyber Threat Environment 162
SAT-04: Security, Compliance and Resilience Training Records 162
Technology Development & Acquisition (TDA) Policy & Standards 164
TDA-01: Technology Development & Acquisition 164
TDA-02: Minimum Viable Product (MVP) Security Requirements 164
TDA-02.1: Minimum Viable Product (MVP) Security Requirements | Ports, Protocols & Services In Use 165
TDA-02.2: Minimum Viable Product (MVP) Security Requirements | Information Assurance Enabled Products 165
TDA-04: Documentation Requirements 166
TDA-04.1: Documentation Requirements | Functional Properties 166
TDA-06: Secure Software Development Practices (SSDP) 167
TDA-07: Secure Development Environments 168
TDA-08: Separation of Development, Testing & Operational Environments 168
TDA-09: Security, Compliance and Resilience Testing Throughout Development 169
TDA-14: Developer Configuration Management 169
Third-Party Management (TPM) Policy & Standards 171
TPM-01: Third-Party Management 171
TPM-04: Third-Party Services 172
TPM-04.2: Third-Party Services | External Connectivity Requirements - Identification of Ports, Protocols & Services 172
TPM-05: Third-Party Contract Requirements 173
TPM-05.2: Third-Party Contract Requirements | Contract Flow-Down Requirements 174
Threat Management (THR) Policy & Standards 175
THR-01: Threat Awareness Program 175
THR-03: Threat Intelligence Feeds 175
THR-05: Insider Threat Awareness 176
Vulnerability & Patch Management (VPM) Policy & Standards 177
VPM-01: Vulnerability & Patch Management Program 177
VPM-02: Vulnerability Remediation Process 177
VPM-04: Continuous Vulnerability Remediation Activities 178
VPM-05: Software & Firmware Patching 178
VPM-06: Vulnerability Scanning 181
VPM-06.1: Vulnerability Scanning | Update Tool Capability 182
VPM-06.3: Vulnerability Scanning | Privileged Access 182

EXAMPLE

WEB SECURITY (WEB) POLICY & STANDARDS 184
WEB-01: WEB SECURITY 184
WEB-02: USE OF DEMILITARIZED ZONES (DMZS) 184
WEB-04: CLIENT-FACING WEB SERVICES 184
GLOSSARY: ACRONYMS & DEFINITIONS 186
ACRONYMS 186
DEFINITIONS 187
RECORD OF CHANGES 188

EXAMPLE

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Consultants, LLP (ACME)'s Technology Assets, Applications and/or Services (TAAS) to protect its data, regardless of where it is stored, transmitted or processed. The following external content is a non-exhaustive list of frameworks that either support the implementation of or are referenced by the NIST 800-171 Compliance Program (NCP):

- The National Institute of Standards and Technology (NIST): [1]
  - NIST AI 100-1: *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
  - NIST AI 600-1: *Trustworthy and Responsible AI*
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-63B, *Digital Identity Guidelines*
  - NIST SP 800-64: *Security Considerations in Secure Development Life Cycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personal Data (PD)*
  - NIST SP 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- The International Organization for Standardization (ISO):[2]
  - ISO/IEC 15288: *Systems and Software Engineering -- System Life Cycle Processes*
  - ISO/IEC 22301: *Societal Security – Business Continuity Management Systems – Requirements*
  - ISO/IEC 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
  - ISO/IEC 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personal Data (PD) in Public Clouds Acting as PD Processors*
  - ISO/IEC 27701: *Information Technology - Security Techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines*
- Other influencing frameworks (alphabetical order):
  - Center for Internet Security (CIS) Critical Security Controls (CSC)[3]
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)[4]
  - Computer Security Incident Handling Guide[5]
  - Control Objectives for Information and Related Technologies (COBIT)[6]
  - Defense Information Systems Agency (DISA) Secure Technology Implementation Guides (STIGs)[7]
  - Department of Defense Cybersecurity Maturity Model Certification (CMMC)[8]
  - Guide to Integrating Forensic Techniques into Incident Response[9]
  - Open Web Application Security Project (OWASP)[10]
  - Payment Card Industry Data Security Standard (PCI DSS)[11]
  - Privacy by Design (PbD) [12]

---

[1] *National Institute of Standards and Technology - https://csrc.nist.gov/publications/sp*
[2] *International Organization for Standardization - https://www.iso.org/home.html*
[3] *Center for Internet Security - https://www.cisecurity.org/*
[4] *Cloud Security Alliance - https://cloudsecurityalliance.org/*
[5] *Computer Security Incident Handling Guide - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final*
[6] *COBIT - https://www.isaca.org/resources/cobit*
[7] *DoD Information Security Agency - https://public.cyber.mil/*
[8] *DoD Cybersecurity Maturity Model Certification - https://www.acq.osd.mil/cmmc/index.html*
[9] *Guide to Integrating Forensic Techniques into Incident Response - https://csrc.nist.gov/publications/detail/sp/800-86/final*
[10] *OWASP - https://owasp.org/*
[11] *Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/*
[12] *Term and principles coined by Dr. Ann Cavoukian - https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*

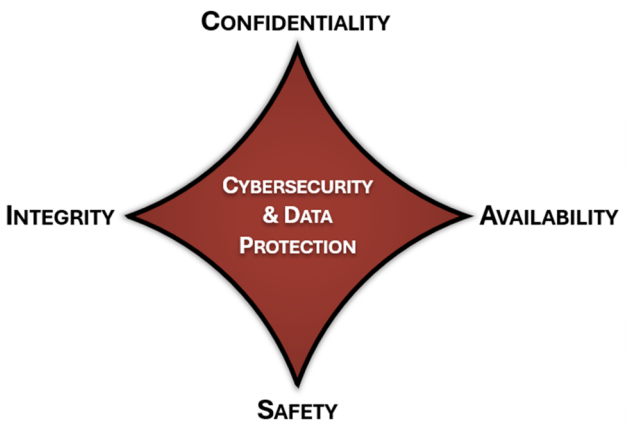
EXAMPLE

MANAGEMENT COMMITMENT

The **NIST 800-171 Compliance Program (NCP)** provides definitive information on the prescribed measures used to establish and enforce the security, compliance and resilience program at ACME Consultants, 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 security, compliance and resilience requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security, compliance and resilience 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 protection of TAASD must include 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 NIST 800-171 Compliance Program (NCP) 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 security, compliance and resilience controls over data and systems that support ACME's operations; and
- Provide for the development, review and maintenance of the security, compliance and resilience 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.

EXAMPLE

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 & Artificial Intelligence (PPTDF-AI) 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

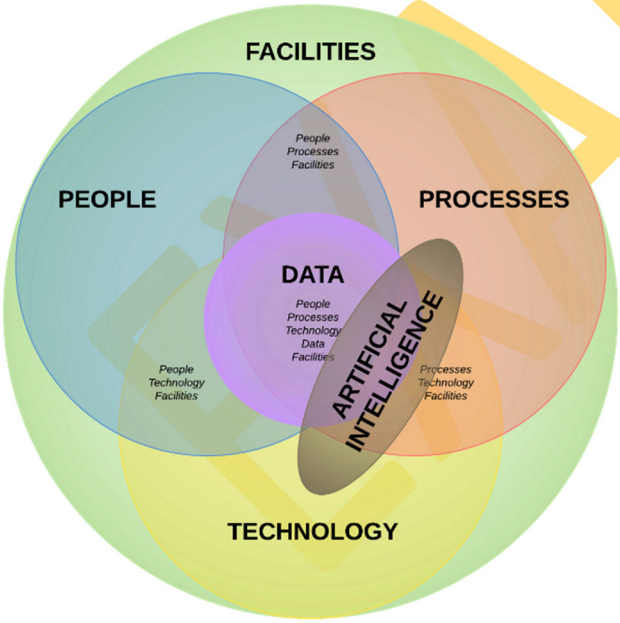
- A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- A network firewall is a device. Therefore, a network firewall is not capable of undergoing end 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, Facilities & Artificial Intelligence (PPTDF-AI) model provides a comprehensive approach to address control applicability. These six (6) components provide a lens to view the applicability of controls.

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

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions must comply with the standards. ACME departments must use these standards or may create a more restrictive standard, but none that are less restrictive, less comprehensive or less compliant than these standards.

SAMPLE

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

ACME's documented roles and responsibilities provides a detailed description of ACME user roles and responsibilities, in regard to cybersecurity-related use obligations.

ACME reserves the right to revoke, change or supplement these policies, standards and guidelines at any time without prior notice. Such changes must be effective immediately upon approval by management unless otherwise stated.

Roles

As part of ACME's Human Resources (HR) department's function to facilitate the implementation of personnel security controls, HR is required to assign all employees and contractors with one, or more, defined roles. Those roles are designed to manage personnel security risk by:

- Assigning a risk designation to all position; and
- Establishing screening criteria for individuals filling those positions

Responsibilities

To ensure an acceptable level of cybersecurity risk, ACME must design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems. The NCP addresses the policies, standards and guidelines.

Data/process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with the NCP's policies, standards and guidelines.

ACME personnel must protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and systems, regardless of how its data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations of Policies, Standards and/or Procedures

Any ACME user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exception To Standards

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception, users must submit a business justification for deviation from the standard in question.

Updates To Policies & Standards

Updates to the NIST 800-171 Compliance Program (NCP) will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

Key Terminology

ACME recognizes two (2) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

EXAMPLE

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[13] and
- NIST Glossary.[14]

From the context of this document, it is important to clarify mandatory versus optional criteria:[15]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

Key terminology to be aware of includes:

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.

Artificial Intelligence and Autonomous Technologies (AI/ML): A term describing tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.

Assessment Boundary. The scope of an entity's control implementation to which assessment of objects is applied:

- An assessment may involve multiple assessment boundaries; and
- Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
- The entire entity;
  - A specific contract, project or initiative;
  - A specific Business Unit (BU) within an entity; or
  - A specific country, or geographic region, of the entity's business operations.

Assessment Objective (AO): A term describing objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.

Assurance. Grounds for justified confidence that a security, compliance and/or resilience claim has been or will be achieved.

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a ACME owns or controls.

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended and that information regarding the equipment is properly documented.

Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

---

[13] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[14] *NIST Glossary - https://csrc.nist.gov/glossary*
[15] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*

EXAMPLE

Compensating Control: A term describing an alternative cybersecurity and/or data protection controls implemented in lieu of the intended control(s) that provide equivalent, or comparable protection.

Conflict of Interest (COI): A term describing situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.

Conformity Assessment. A demonstration that specified requirements are fulfilled.

Control: A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Inheritance: A term describing a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align ACME with accepted due diligence and due care requirements.

Controlled Unclassified Information (CUI): A term describing a type of information that requires safeguarding, or dissemination controls, pursuant to and consistent with applicable United States (US) law, regulations, and US Government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act.[16] While CUI is unclassified, it requires control to prevent the release of information that, if aggregated with other sources of information, could reveal exploitable information to adversaries.

Cybersecurity/Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. *Annex 1: Data Classification & Handling Guidelines* provides guidance on data classification and handling restrictions.

Data Controller. A term describing the data privacy stakeholder (or data privacy stakeholders) that determines the purposes and means for processing Personal Data (PD) other than natural persons who use data for personal purposes.

Data Principle. A term describing the natural person to whom the Personal Data (PD) relates.

Data Processor. A term describing the data privacy stakeholder that processes Personal Data (PD) on behalf of and in accordance with the instructions of a PD controller.

Discretionary Security Requirements (DSR). A term describing discretionary cybersecurity and/or data privacy controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.

Due Care. The standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used in a tort action to determine whether a person was negligent. [17]

Due Diligence. The level of reasonable care or attention expected to avoid liability. [18]

---

[16] *N US National Archives (NARA) - https://www.archives.gov/cui/about*
[17] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_care*
[18] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_diligence*

EXAMPLE

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Enduring Exception: A term describing a special circumstance or system where remediation and full compliance with a statutory, regulatory or other compliance-related requirement is not feasible.

External Service Provider (ESP): A term describing an independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to:

- Consulting / professional services;
- Software development;
- Staff augmentation; and
- Technology support (e.g., Managed Services Provider (MSP)).

Evidence Request List (ERL): A term describing a finite list of supporting evidence used in an audit or assessment.

Federal Contract Information (FCI): A term describing a type of information that is not intended for public release. FCI is provided by, or generated for, the US Government under a contract to develop, or deliver, a product or service to the US Government. This does not include information provided by the US Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.[19]

Guidelines: A term describing recommended practices that are based on industry-recognized secure practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

Implemented Capability. An implemented capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.

Information Assurance: A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

Information Technology (IT). A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Loss. A negative impact from an incident that can be categorized as:

- Productivity loss;
- Data loss;
- Financial loss; and/or
- Reputation loss.

Material Control. A term describing a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data privacy control that:

- It is not capable of having compensating controls; and
- Its absence, or failure, exposes an organization to such a degree that it could have a material impact.

Material Risk. A term describing an identified risk that poses a material impact. A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.).

---

[19] *FAR 52.204-21 - https://www.acquisition.gov/far/52.204-21*

EXAMPLE

Material Threat. A term describing an identified threat poses a material impact. A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.).

Material Incident. A term describing an incident that poses a material impact. A material incident is an occurrence that does or has the potential to:

- Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
- Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).

Material Weakness. A term describing a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.

Minimum Compliance Requirements (MCR): A term describing the minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.

Maturity Level Criteria (MLC): A term describing the specific criteria for each maturity level to define reasonable staffing, technologies and processes to implement a desired level of maturity.

Mechanism. A mechanism can be described as a:

- Process or system that is used to produce a particular result; or
- Device or method for achieving a security-relevant purpose.

Personal Data (PD) /Personal Information (PI). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[20]

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Process Owner/Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, process or the data hosted on the asset or process. It does not mean that the asset belongs to the owner in a legal sense. Data/process owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.

Responsible, Accountable, Supportive, Consulted & Informed (RASCI): A term describing a RASCI matrix that defines responsibilities associated with individuals or teams:

- Responsible - entity directly responsible for performing a task (e.g., control/process operator);
- Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner);
- Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task;
- Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and
- Informed - entity(ies) not involved in task execution but are informed when the task is completed.

Risk. A risk is:

- A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or

[20] *European Union General Data Protection Requirement – Article 4(1)*

EXAMPLE

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.[36]

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.

---

[36] *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)*

EXAMPLE

Guidelines: System components are discrete, identifiable information TAAS that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces.

AST-02.1: Asset Inventories | Updates During Installations/Removals

Control Objective: The organization updates asset inventories as part of component installations, removals and asset upgrades.[37]

Standard: Where technically feasible, data/process owners and asset custodians must update the inventory of system components as an integral part of component installations, removals and system updates.

Guidelines: None

AST-02.3: Asset Inventories | Component Duplication Avoidance

Control Objective: The organization establishes and maintains an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.[38]

Standard: Where technically feasible, data/process owners and asset custodians must verify that system components are not duplicated in other asset inventories.

Guidelines: This control addresses the potential problem of duplicate accounting of system components in large or complex interconnected systems.

AST-05: Security of Assets & Media

Control Objective: The organization maintains strict control over the internal or external distribution of any kind of sensitive/regulated media.[39]

Standard: Data/process owners and asset custodians must maintain strict control over the internal or external distribution of sensitive assets or media, including the following:

(a) Classifying media in accordance with *Annex 1: Data Classification & Handling Guidelines* so the sensitivity of the data can be determined;
(b) Sending sensitive media by secured courier or another delivery method that can be accurately tracked; and
(c) Ensuring prior management approval for any and all media that is moved from a secured area (including when media is distributed to individuals).

---

[37] *NIST SP 800-53 R5: CM-8(1) | NIST SP 800-171 R3: 03.04.10.a, 03.04.10.b, 03.04.10.c*
[38] *NIST SP 800-53 R5: CM-8 | NIST SP 800-171 R2: NFO - CM-8(5)*
[39] *ISO 27002-2022: 7.9 | NIST SP 800-171 R2: NFO - MP-1 | NIST SP 800-171 R3: 03.07.04.a*

EXAMPLE

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change in a unified effort to prevent business disruptions and unintended outcomes. Without properly documented and implemented change controls, security, compliance and resilience features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise that affect Technology Assets, Applications, Services and/or Data (TAASD).

Policy: ACME shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change affecting production Technology Assets, Applications, Services and/or Data (TAASD).

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

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of change management controls.[47]

Standard: ACME's Change Management Program requires data/process owners and asset custodians to test, validate and document changes to systems before implementing the changes on the production network. Changes for any production Technology Assets, Applications and/or Services (TAAS) must:

(a) Be:
    1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;
    2. Approved by a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
    3. Approved by ACME's Change Control Board (CCB);

(b) Sufficiently document the following criteria to enable independent review:
    1. Reason for, and description of, the change;
    2. Security impact;
    3. Change approval by authorized parties;
    4. Functionality testing to verify the change:
        i. Did not adversely impact the security of the network; and
        ii. Performs as expected;
    5. For bespoke and custom software changes, all updates are tested for compliance with applicable statutory, regulatory and contractual obligations; and
    6. Procedures to address failures and return to a secure state;

(c) Ensure all applicable statutory, regulatory and contractual requirements are confirmed to be in place on all new or changed systems and networks; and

(d) As applicable, update affected documentation to include the changes to prevent inconsistencies between network documentation and the actual configuration.

Guidelines: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality or data privacy or any combination thereof.

Due to the constantly changing state of pre- production environments, they are often less secure than the production environment. Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

---

[47] *ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a | CSF 2.0: ID.RA-07*

EXAMPLE

Pre-production environments include development, testing, User Acceptance Testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre-production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

CHG-02: Configuration Change Control

Control Objective: The organization governs the technical configuration change control processes.[48]

Standard: Data/process owners and asset custodians must follow ACME's change control processes and procedures for all changes to system components:

(a) Utilize separate environments for development/testing/staging and production;
(b) Utilize a separation of duties between development/testing/staging and production environments;
(c) Prohibit the use of production data (e.g., live data) for testing or development;
(d) Remove test data and accounts before production systems become active/goes into production; and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following:
    1. Documentation of impact;
    2. Documented change approval by authorized parties; and
    3. Functionality testing to verify that the change does not adversely impact the security of the system;
(f) Back-out procedures; and
(g) Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed systems and networks and documentation updated as applicable.

Guidelines: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers and mobile devices), unscheduled/unauthorized changes and changes to remediate vulnerabilities.

CHG-02.2: Configuration Change Control | Test, Validate & Document Changes

Control Objective: The organization tests and documents proposed changes in a non-production environment before changes are implemented in a production environment.[49]

Standard: Data/process owners and asset custodians must:

(a) Where technically feasible, test and validate configuration changes in a test environment, prior to deploying the change in the production environment; and
(b) Document the changes that were implemented in the production environment.

Guidelines: When operating platforms are changed, mission-critical (SC1) and business-critical (SC2) Technology Assets, Applications and/or Services (TAAS) should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. If it is not technically or logistically feasible to test a configuration change, compensating control should be identified and implemented in order to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include, but is not limited to:

- Images of systems;
- Backups of configurations;
- Viable back out plan;
- After-hours implementation; and
- Pilot/test group rollouts.

---

[48] *ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a, 03.04.03.b, 03.04.03.c | NIST CSF 2.0: ID.RA-07*

[49] *ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3(2), CM-3(7), SA-8(31) | NIST SP 800-171 R2: NFO - CM-3(2) | NIST SP 800-171 R3: 03.04.03.b, 03.04.03.c, 03.04.04.a, 03.04.11.b | NIST CSF 2.0: ID.RA-07*

EXAMPLE

- NCP SUPPLEMENTAL DOCUMENTATION -

ANNEXES, TEMPLATES & REFERENCES

EXAMPLE

INTERNAL USE
Access Limited to Internal Use Only

Table of Contents

Annexes 4

Annex 1: Data Classification & Handling Guidelines 4

Data Classification 4

Labeling 6

General Assumptions 6

Personal Data (PD) 6

Sensitive Personal Data (sPD) 7

Data Handling Guidelines 8

Annex 2: Data Classification Examples 11

Annex 3: Data Retention Schedule 13

Annex 4: Baseline Security Categorization Guidelines 15

Safety & Criticality 15

Basic Assurance Requirements 16

Enhanced Assurance Requirements 16

Annex 5: Rules of Behavior (Acceptable & Unacceptable Use) 17

Acceptable Use 17

Prohibited Use 17

Additional Rules For Security & Privileged Users 18

Annex 6: Guidelines for Personal Use of Organizational IT Resources 19

Annex 7: Risk Management Framework (RMF) 20

Risk Management Overview 20

Risk Management Framework (RMF) 20

Assessing Risk 22

Annex 8: System Hardening 23

Server-Class Systems 23

Workstation-Class Systems 23

Network Devices 23

Mobile Devices 23

Databases 24

Annex 9: Safety Considerations With Embedded Technology 25

Mission Critical (SC-1) 25

Business Critical (SC-2) 25

Non-Critical (SC-3) & Business Supporting (SC-4) 25

Annex 10: Indicators of Compromise (IoC) 26

Templates 29

Template 1: Management Directive (Policy Authorization) 29

Template 2: User Acknowledgement Form 30

Template 3: User Equipment Receipt of Issue 31

Template 4: Service Provider Non-Disclosure Agreement (NDA) 32

Template 5: Incident Response Plan (IRP) 33

Plan Objectives 33

Incident Discovery 33

Common Effects of Attacks 36

Incident Response Stages 37

Incident Categories 38

Escalation Level Considerations 40

Incident Response Process 41

Incident Response Team (24x7) 43

Incident Response Team Capabilities 43

Incident Notification Requirements 43

Post Incident Requirements 44

Template 6: Incident Response Form 45

Template 7: Appointment Orders (Information Security Officer) 45

Template 8: Privileged User Account Request Form 47

Template 9: Change Management Request Form 48

Template 10: Change Control Board (CCB) Meeting Minutes 50

EXAMPLE

Template 11: Plan of Action & Milestones (POA&M) / Risk Register **51**
Template 12: Ports, Protocols & Services (PPS) **52**
Template 13: Business Impact Analysis (BIA) **53**
Template 14: Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP) **55**
Disaster Recovery Plan (DRP) *55*
Business Continuity Plan (BCP) *56*
Critical Equipment *58*
Alternate Work Site *58*
Assumed Risk & Maximum Downtime Requirements *58*
Template 15: Privacy Impact Assessment (PIA) **59**
Template 16: Memorandum For Record (MFR) – Defining CUI **61**
References **62**
Reference 1: Exception Request Process **62**
Reference 2: Electronic Discovery (eDiscovery) Guidelines **63**
Federal Rules of Civil Procedure (FCRP) *63*
Legal Hold *63*
Electronic Discovery *63*
Reference 3: Types of Security Controls **64**
Preventative Controls *64*
Detective Controls *64*
Corrective Controls *64*
Recovery Controls *64*
Directive Controls *64*
Deterrent Controls *64*
Compensating Controls *64*
Reference 4: Information Security Management System (ISMS) **65**
Cybersecurity Program - Plan *65*
Cybersecurity Program - Do *65*
Cybersecurity Program - Check *65*
Cybersecurity Program - Act *65*
Reference 5: Cybersecurity Roles & Responsibilities Overview **66**
Cybersecurity Role Categories *66*
Cybersecurity Specialty Areas (Roles) *66*
Cybersecurity Work Roles & Responsibilities *68*

EXAMPLE

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following seven (7) sensitivity levels:

CUI-Restricted	CUI - RESTRICTED Access Limited to Authorized Personnel Controlled Unclassified Information (CUI)
Sensitive Personal Data (sPD)-Restricted	sPD - RESTRICTED Access Limited to Authorized Personnel
Personal Data (PD)-Restricted	PD - RESTRICTED Access Limited to Authorized Personnel
Restricted	RESTRICTED Access Limited to Authorized Personnel
Sensitive	SENSITIVE Access Limited to Authorized Personnel
Internal Use	INTERNAL USE Access Limited to Internal Use Only
Public	PUBLIC Public Release Authorized

Classification		Data Sensitivity Description
Controlled Unclassified Information (CUI) - Restricted	**Definition**	CUI-Restricted information is U.S. Government regulated data that is highly-sensitive business information and the level of protection is dictated externally by both NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI-Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if CUI-Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company's reputation.

EXAMPLE

Sensitive Personal Data (sPD) Restricted	**Definition**	Sensitive Personal Data (sPD) is a subset of Personal Data (PD) that is highly-sensitive information about individuals (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. sPD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the sPD is authorized to be stored, processed and/or transmitted.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if sPD Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements, damaging the company's reputation and posing a risk to identified individuals (e.g., identity theft, stalking, harassment, etc.).
Personal Data (PD) Restricted	**Definition**	Personal Data (PD) Restricted that is information that can identify an individual (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. The difference between sPD Restricted and PD Restricted is that PD Restricted information is publicly-available information (e.g., social media, news, court filings, etc.). PD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the PD Restricted is authorized to be stored, processed and/or transmitted, unless it is publicly-available information.
	Potential Impact of Loss	**· MODERATE DAMAGE would occur if PD Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company's reputation.**
Restricted	**Definition**	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is generally dictated externally by statutory, regulatory and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements and posing an identity theft risk.
Sensitive	**Definition**	Sensitive information is highly-valuable, sensitive business information and the level of protection is dictated internally by ACME.
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Sensitive information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, damaging the company's reputation and violating contractual requirements.
Internal Use	**Definition**	Internal Use information is information originated or owned by ACME or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME. · Impact could include damaging the company's reputation and violating contractual requirements.
Public	**Definition**	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.

	Potential Impact of Loss	· NO DAMAGE would occur if public information were to become available to parties either internal or external to ACME. · Impact would not be damaging or a risk to business operations.

LABELING

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
- **Displayed**. CUI-Restricted, Restricted or Sensitive information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

GENERAL ASSUMPTIONS

- Any information created or received by ACME employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Sensitive information, the entire application is Sensitive.
- Restricted, Sensitive and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

PERSONAL DATA (PD)

PD is any information about an individual maintained by ACME including any information that:

- Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD.

Examples of PD in the United States (US) include, but are not limited to: [1]

- An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social security number.
  - Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
  - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  - Medical information.
  - Health insurance information.
  - Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

[1] *CA Civil Code 1798.81.5 - https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5*

EXAMPLE

- A username or email address in combination with a password or security question and answer that would permit access to an online account.

Examples of PD outside of the US include, but are not limited to: [2]

Article 4, Section 1 of the EU General Data Protection Regulation (GDPR) defines "personal data" as:

- Any information relating to an identified or identifiable natural person ('data subject');
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:
  - A name;
  - An identification number;
  - Location data;
  - An online identifier; or
  - To one or more factors specific to the:
    - Physical;
    - Physiological;
    - Genetic;
    - Mental;
    - Economic;
    - Cultural; or
    - Social identity of that natural person.

SENSITIVE PERSONAL DATA (SPD)

Per the US National Archives (NARA), "sensitive PD" is defined as "*A subset of PD that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual*." Some forms of PD are sensitive as stand-alone elements.

- Examples of stand-alone PD include Social Security Numbers (SSN), driver's licenses or state identification numbers; Alien Registration Numbers; financial account numbers; and biometric identifiers such as fingerprint, voiceprint, or iris scans.
- Additional examples of SPD include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:
  - Truncated SSN (such as last four digits);
  - Date of birth (month, day, and year);
  - Citizenship or immigration status;
  - Ethnic or religious affiliation;
  - Sexual orientation;
  - Criminal history;
  - Medical information; and
  - System authentication information such as mother's maiden name, account passwords, or personal identification numbers.
- Other PD may be "sensitive" depending on its context, such as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PD but is not sensitive.

Note: Per NARA's CUI Program, Sensitive PD is considered CUI[3]

[2] *EU GDPR Article 4, Section 1*

[3] *NARA Sensitive PD - https://www.archives.gov/cui/registry/category-detail/sensitive-personally-identifiable-info*

EXAMPLE

DATA HANDLING GUIDELINES

Note: For U.S. Government regulated data, the following requirements supersede ACME data handling guidelines:

- *For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handing:*
  - *48 CFR 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))*
- *For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handing:*
  - *32 CFR Part 170*
  - *DoD Instruction 5200.48*
  - *NIST SP 800-171*

Handling Controls	CUI - RESTRICTED	Restricted	Sensitive	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non- employees.	▪ NDA is required prior to access by non- employees.	▪ NDA is recommended prior to access by non-employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups

EXAMPLE

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Sensitive	Restricted	PD - Restricted	sPD - Restricted	CUI - Restricted
Non-Public Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Social Security Number (SSN)						X	
	Employer Identification Number (EIN)						X	
	Driver's License (DL) Number						X	
	Financial Account Number						X	
	Payment Card Number (credit or debit)						X	
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)						X	
	Geolocation Information (e.g., precise geographic location and/or history)						X	
	Race / Ethnicity						X	
	Religious Affiliation						X	
	Union Membership						X	
	Philosophical Beliefs						X	
	Private Communications (e.g., contents of private mail, emails and text messages)						X	
	Genetic Information						X	
	Biometrics						X	
	Health Information						X	
	Sexual Orientation						X	
	Birth Date						X	
	First & Last Name						X	
	Age						X	
	Phone Number						X	
	Home Address						X	
	Gender						X	
	Email Address						X	
Publicly Available Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Geolocation Information (e.g., precise geographic location and/or history)					X		
	Race / Ethnicity					X		
	Religious Affiliation					X		
	Union Membership					X		
	Philosophical Beliefs					X		
	Private Communications (e.g., contents of private mail, emails and text messages)					X		
	Health Information					X		
	Sexual Orientation					X		
	Birth Date					X		

EXAMPLE

ANNEX 3: DATA RETENTION SCHEDULE

The following schedule highlights suggested retention periods* for some of the major categories of data:
** Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)*

CATEGORY	TYPE OF RECORD	RETENTION PERIOD
Business Records	Amendments	Permanent
	Annual Reports	Permanent
	Articles of Incorporation	Permanent
	Board of Directors (elections, minutes, committees, etc.)	Permanent
	Bylaws	Permanent
	Capital stock & bond records	Permanent
	Charter	Permanent
	Contracts & agreements	Permanent
	Copyrights	Permanent
	Correspondence (General)	5
	Correspondence (Legal)	Permanent
	Partnership agreement	Permanent
	Patents	Permanent
	Service marks	Permanent
	Stock transfers	Permanent
	Trademarks	Permanent
CATEGORY	**TYPE OF RECORD**	**RETENTION PERIOD**
Financial Records	Audit report (external)	Permanent
	Audit report (internal)	3
	Balance sheets	Permanent
	Bank deposit slips, reconciliations & statements	7
	Bills of lading	3
	Budgets	3
	Cash disbursement & receipt record	7
	Checks (canceled)	3
	Credit memos	3
	Depreciation schedule	7
	Dividend register & canceled dividend checks	Permanent
	Employee expense reports	3
	Employee payroll records (W-2, W-4, annual earnings records, etc.)	7
	Financial statements (annual)	Permanent
	Freight bills	3
	General ledger	Permanent
	Internal reports (work orders, sales reports, production reports)	3
	Inventory lists	3
	Investments (sales & purchases)	Permanent
	Profit / Loss statements	Permanent
	Purchase and sales contracts	3
	Purchase order	3
	Subsidiary ledgers (accounts receivable, accounts payable, etc.)	Permanent
	Tax returns	Permanent
	Vendor Invoices	7
	Worthless securities	7

EXAMPLE

ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL)*.

SAFETY & CRITICALITY

One component of assessing risk is to understand the criticality of systems and data. By having a clear understanding of the Safety & Criticality Level (SC) for an asset, system, application, service or data, determining potential impact will be more accurate.

There are four (4) SC levels:

1. Mission Critical (SC1);
2. Business Critical (SC2);
3. Non-Critical (SC3); and
4. Business Supporting (SC4).

MISSION CRITICAL (SC1)

Mission Critical (SC1) assets handle information that is determined to be vital to the operations or mission effectiveness of ACME.

The impact of a SC1 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide business stoppage with significant revenue impact can be anything that creates a significant impact on ACME's ability to perform its mission;
- Public, wide-spread damage to ACME's reputation;
- Direct, negative & long-term impact on customer satisfaction; and
- Risk to human health or the environment.

Examples of SC1 systems, applications and services include, but are not limited to:

- *Enterprise Resource Management (ERM) system (e.g., SAP)*
- *Active Directory (AD)*
- *Ability to process Point of Sale (PoS) or eCommerce payments*

BUSINESS CRITICAL (SC2)

Business Critical (SC2) assets handle information that is important to the support of ACME's primary operations.

The impact of a SC2 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide delay or degradation in providing important support services that may seriously impact mission effectiveness or the ability to operate;
- Department-level business stoppage with direct or indirect revenue impact; and
- Direct, negative & short-term impact on customer satisfaction.

Examples of SC2 systems, applications and services include, but are not limited to:

- *Email (e.g., Exchange)*
- *Payroll systems*
- *Corporate website functionality*
- *Corporate mobile device application functionality*
- *HVAC systems*
- *Customer support / call center functionality*

NON-CRITICAL (SC3)

Non-Critical (SC3) assets handle information that is necessary for the conduct of day-to-day business, but they are not mission critical in the short-term.

The impact of a SC3 system, or its data, being unavailable includes, but is not limited to:

- Widespread delays or degradation of services or routine activities;
- Widespread employee productivity degradation;

EXAMPLE