

YOUR LOGO GOES HERE

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

ISO 27001 & 27002

ACME Professional Services, LLC



INTERNAL USE

Access Limited to Internal Use Only

***IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES
WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)***

TABLE OF CONTENTS

CYBERSECURITY AND DATA PROTECTION PROGRAM (CDPP) OVERVIEW	9
INTRODUCTION	9
SECURE CONTROLS FRAMEWORK (SCF) STRUCTURE	9
PURPOSE	9
SCOPE & APPLICABILITY	10
POLICY OVERVIEW	10
VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES	10
EXCEPTION TO STANDARDS	10
UPDATES TO POLICIES & STANDARDS	11
KEY TERMINOLOGY	11
CYBERSECURITY & DATA PROTECTION PROGRAM STRUCTURE	13
MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION	13
POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	13
CYBERSECURITY & PRIVACY GOVERNANCE (GOV) POLICY & STANDARDS	14
GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM	14
<i>GOV-01.1: DIGITAL SECURITY GOVERNANCE PROGRAM STEERING COMMITTEE</i>	14
<i>GOV-01.2: DIGITAL SECURITY GOVERNANCE PROGRAM STATUS REPORTING TO GOVERNING BODY</i>	14
GOV-02: PUBLISHING CYBERSECURITY & PRIVACY DOCUMENTATION	15
GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY & PRIVACY PROGRAM	15
GOV-04: ASSIGNED CYBERSECURITY & PRIVACY RESPONSIBILITIES	15
GOV-05: MEASURES OF PERFORMANCE	16
GOV-06: CONTACTS WITH AUTHORITIES	16
GOV-07: CONTACTS WITH GROUPS & ASSOCIATIONS	16
GOV-08: DEFINED BUSINESS CONTEXT & MISSION	17
GOV-09: DEFINED CONTROL OBJECTIVES	17
ASSET MANAGEMENT (AST) POLICY & STANDARDS	18
AST-01: ASSET GOVERNANCE	18
<i>AST-01.1: ASSET GOVERNANCE ASSET-SERVICE DEPENDENCIES</i>	18
<i>AST-01.2: ASSET GOVERNANCE STAKEHOLDER IDENTIFICATION & INVOLVEMENT</i>	19
AST-02: ASSET INVENTORIES	19
<i>AST-02.7: ASSET INVENTORIES SOFTWARE LICENSING RESTRICTIONS</i>	19
<i>AST-02.8: ASSET INVENTORIES DATA ACTION MAPPING</i>	20
AST-03: ASSET OWNERSHIP ASSIGNMENT	20
<i>AST-03.1: ASSIGNING OWNERSHIP OF ASSETS ACCOUNTABILITY INFORMATION</i>	20
<i>AST-03.2: ASSIGNING OWNERSHIP OF ASSETS PROVENANCE</i>	20
AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	21
<i>AST-04.1: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) ASSET SCOPE CLASSIFICATION</i>	22
AST-05: SECURITY OF ASSETS & MEDIA	23
AST-06: UNATTENDED END-USER EQUIPMENT	23
AST-07: KIOSKS & POINT OF INTERACTION (POI) DEVICES	23
AST-08: TAMPER DETECTION	24
AST-09: SECURE DISPOSAL, DESTRUCTION OR RE-USE OF EQUIPMENT	25
AST-10: RETURN OF ASSETS	25
AST-11: REMOVAL OF ASSETS	25
AST-12: USE OF PERSONAL DEVICES	26
AST-15: TAMPER PROTECTION	26
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) POLICY & STANDARDS	27
BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	27
<i>BCD-01.1: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH RELATED PLANS</i>	27
<i>BCD-01.2: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH EXTERNAL SERVICE PROVIDERS</i>	28
BCD-04: CONTINGENCY PLAN TESTING & EXERCISES	28
BCD-08: ALTERNATE STORAGE SITE	28
BCD-09: ALTERNATE PROCESSING SITE	29
BCD-11: DATA BACKUPS	29
<i>BCD-11.1: DATA BACKUPS TESTING FOR RELIABILITY & INTEGRITY</i>	31
<i>BCD-11.2: DATA BACKUPS SEPARATE STORAGE FOR CRITICAL INFORMATION</i>	31

BCD-11.4: DATA BACKUPS CRYPTOGRAPHIC PROTECTION	31
BCD-11.7: DATA BACKUPS REDUNDANT SECONDARY SYSTEM	32
CAPACITY & PERFORMANCE PLANNING (CAP) POLICY & STANDARDS	33
CAP-01: CAPACITY & PERFORMANCE MANAGEMENT	33
CAP-03: CAPACITY PLANNING	33
CHANGE MANAGEMENT (CHG) POLICY & STANDARDS	34
CHG-01: CHANGE MANAGEMENT PROGRAM	34
CHG-02: CONFIGURATION CHANGE CONTROL	34
CHG-02.2: CONFIGURATION CHANGE CONTROL TEST, VALIDATE & DOCUMENT CHANGES	35
CLOUD SECURITY (CLD) POLICY & STANDARDS	36
CLD-01: CLOUD SERVICES	36
CLD-02: CLOUD SECURITY ARCHITECTURE	36
CLD-04: APPLICATION & PROGRAM INTERFACE (API) SECURITY	37
CLD-06: MULTI-TENANT ENVIRONMENTS	37
CLD-06.1: MULTI-TENANT ENVIRONMENTS CUSTOMER RESPONSIBILITY MATRIX (CRM)	37
CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS	37
COMPLIANCE (CPL) POLICY & STANDARDS	39
CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	39
CPL-01.1: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE NON-COMPLIANCE OVERSIGHT	39
CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE COMPLIANCE SCOPE	39
CPL-02: SECURITY & PRIVACY CONTROLS OVERSIGHT	40
CPL-02.1: SECURITY CONTROLS OVERSIGHT INTERNAL AUDIT FUNCTION	41
CPL-03: SECURITY ASSESSMENTS	41
CPL-03.1: SECURITY ASSESSMENTS INDEPENDENT ASSESSORS	41
CPL-03.2: SECURITY ASSESSMENTS FUNCTIONAL REVIEW OF SECURITY CONTROLS	42
CPL-04: AUDIT ACTIVITIES	42
CONFIGURATION MANAGEMENT (CFG) POLICY & STANDARDS	43
CFG-01: CONFIGURATION MANAGEMENT PROGRAM	43
CFG-01.1: CONFIGURATION MANAGEMENT PROGRAM ASSIGNMENT OF RESPONSIBILITY	43
CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS	43
CFG-02.1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS REVIEWS & UPDATES	45
CFG-02.4: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS DEVELOPMENT & TEST ENVIRONMENTS	45
CFG-02.5: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS	45
CFG-03: LEAST FUNCTIONALITY	46
CFG-03.1: LEAST FUNCTIONALITY PERIODIC REVIEW	46
CONTINUOUS MONITORING (MON) POLICY & STANDARDS	47
MON-01: CONTINUOUS MONITORING	47
MON-01.1: CONTINUOUS MONITORING INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)	48
MON-01.2: CONTINUOUS MONITORING AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	48
MON-01.3: CONTINUOUS MONITORING INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC	48
MON-01.4: CONTINUOUS MONITORING SYSTEM GENERATED ALERTS	49
MON-01.8: CONTINUOUS MONITORING REVIEWS & UPDATES	49
MON-02: CENTRALIZED EVENT LOG COLLECTION	49
MON-02.1: CENTRALIZED SECURITY EVENT LOG COLLECTION CORRELATE MONITORING INFORMATION	50
MON-02.2: CENTRALIZED SECURITY EVENT LOG COLLECTION CENTRAL REVIEW & ANALYSIS	50
MON-03: CONTENT OF AUDIT RECORDS	50
MON-03.3: CONTENT OF AUDIT RECORDS PRIVILEGED FUNCTIONS LOGGING	51
MON-06: MONITORING REPORTING	51
MON-08: PROTECTION OF EVENT LOGS	52
MON-11: MONITORING FOR INFORMATION DISCLOSURE	52
MON-11.3: MONITORING FOR INFORMATION DISCLOSURE MONITORING FOR INDICATORS OF COMPROMISE (IOC)	52
CRYPTOGRAPHIC PROTECTIONS (CRY) POLICY & STANDARDS	54
CRY-01: USE OF CRYPTOGRAPHIC CONTROLS	54
CRY-01.2: USE OF CRYPTOGRAPHIC CONTROLS EXPORT-CONTROLLED TECHNOLOGY	54
CRY-03: TRANSMISSION CONFIDENTIALITY	54

CRY-04: TRANSMISSION INTEGRITY	55
CRY-05: ENCRYPTING DATA AT REST	55
CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT	56
CRY-09.3: CRYPTOGRAPHIC KEY MANAGEMENT CRYPTOGRAPHIC KEY LOSS OR CHANGE	58
CRY-09.4: CRYPTOGRAPHIC KEY MANAGEMENT CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS	58
DATA CLASSIFICATION & HANDLING (DCH) POLICY & STANDARDS	60
DCH-01: DATA PROTECTION	60
DCH-02: DATA & ASSET CLASSIFICATION	60
DCH-03: MEDIA ACCESS	61
DCH-03.2: MEDIA ACCESS MASKING DISPLAYED DATA	61
DCH-04: MEDIA MARKING	61
DCH-06: MEDIA STORAGE	61
DCH-07: MEDIA TRANSPORTATION	62
DCH-07.1: MEDIA TRANSPORTATION CUSTODIANS	62
DCH-07.2: MEDIA TRANSPORTATION ENCRYPTING DATA IN STORAGE MEDIA	62
DCH-08: PHYSICAL MEDIA DISPOSAL	63
DCH-09: DIGITAL MEDIA SANITIZATION	63
DCH-09.1: MEDIA SANITIZATION MEDIA SANITIZATION DOCUMENTATION	64
DCH-09.3: MEDIA SANITIZATION SANITIZATION OF PERSONAL DATA (PD)	64
DCH-10: MEDIA USE	64
DCH-10.1: MEDIA USE LIMITATIONS ON USE	65
DCH-12: REMOVABLE MEDIA SECURITY	65
DCH-14: INFORMATION SHARING	65
DCH-17: AD-HOC TRANSFERS	65
DCH-18: MEDIA & DATA RETENTION	66
DCH-21: INFORMATION DISPOSAL	67
DCH-23: DE-IDENTIFICATION (ANONYMIZATION)	67
DCH-23.4: DE-IDENTIFICATION (ANONYMIZATION) REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS	68
ENDPOINT SECURITY (END) POLICY & STANDARDS	69
END-01: ENDPOINT SECURITY	69
END-02: ENDPOINT PROTECTION MEASURES	69
END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	70
END-03.2: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS GOVERNING ACCESS RESTRICTION FOR CHANGE	70
END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	70
END-04.1: MALICIOUS CODE PROTECTION (ANTI-MALWARE) AUTOMATIC ANTIMALWARE SIGNATURE UPDATES	71
HUMAN RESOURCES SECURITY (HRS) POLICY & STANDARDS	72
HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	72
HRS-02: POSITION CATEGORIZATION	72
HRS-03: ROLES & RESPONSIBILITIES	72
HRS-03.1: ROLES & RESPONSIBILITIES USER AWARENESS	73
HRS-03.2: ROLES & RESPONSIBILITIES COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS	73
HRS-04: PERSONNEL SCREENING	73
HRS-04.1: PERSONNEL SCREENING ROLES WITH SPECIAL PROTECTION MEASURES	74
HRS-04.2: PERSONNEL SCREENING FORMAL INDOCTRINATION	74
HRS-05: TERMS OF EMPLOYMENT	74
HRS-05.1: TERMS OF EMPLOYMENT RULES OF BEHAVIOR	74
HRS-05.2: TERMS OF EMPLOYMENT SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS	75
HRS-05.3: TERMS OF EMPLOYMENT USE OF COMMUNICATIONS TECHNOLOGY	75
HRS-05.4: TERMS OF EMPLOYMENT USE OF CRITICAL TECHNOLOGIES	75
HRS-05.5: TERMS OF EMPLOYMENT USE OF MOBILE DEVICES	76
HRS-05.7: TERMS OF EMPLOYMENT POLICY FAMILIARIZATION & ACKNOWLEDGEMENT	76
HRS-06: ACCESS AGREEMENTS	76
HRS-06.1: ACCESS AGREEMENTS CONFIDENTIALITY AGREEMENTS	77
HRS-07: PERSONNEL SANCTIONS	77
HRS-07.1: PERSONNEL SANCTIONS WORKPLACE INVESTIGATIONS	77
HRS-08: PERSONNEL TRANSFER	78

HRS-09: PERSONNEL TERMINATION	78
<i>HRS-09.3: PERSONNEL TERMINATION POST-EMPLOYMENT REQUIREMENTS</i>	78
HRS-11: SEPARATION OF DUTIES (SOD)	78
HRS-12: INCOMPATIBLE ROLES	79
IDENTIFICATION & AUTHENTICATION (IAC) POLICY & STANDARDS	80
IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	80
IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	80
IAC-03: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS	81
IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	81
IAC-05: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES	81
IAC-07: USER PROVISIONING & DE-PROVISIONING	82
<i>IAC-07.1: USER PROVISIONING & DE-PROVISIONING CHANGE OF ROLES & DUTIES</i>	82
<i>IAC-07.2: USER PROVISIONING & DE-PROVISIONING TERMINATION OF EMPLOYMENT</i>	83
IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	83
IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)	84
<i>IAC-09.1: IDENTIFIER MANAGEMENT USER IDENTITY (ID) MANAGEMENT</i>	84
<i>IAC-09.4: IDENTIFIER MANAGEMENT CROSS-ORGANIZATION MANAGEMENT</i>	84
IAC-10: AUTHENTICATOR MANAGEMENT	85
<i>IAC-10.1: AUTHENTICATOR MANAGEMENT PASSWORD-BASED AUTHENTICATION</i>	85
<i>IAC-10.5: AUTHENTICATOR MANAGEMENT PROTECTION OF AUTHENTICATORS</i>	87
<i>IAC-10.8: AUTHENTICATOR MANAGEMENT VENDOR-SUPPLIED DEFAULTS</i>	87
<i>IAC-10.11: AUTHENTICATOR MANAGEMENT PASSWORD MANAGERS</i>	88
IAC-15: ACCOUNT MANAGEMENT	88
<i>IAC-15.1: ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT</i>	89
<i>IAC-15.2: ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS</i>	89
<i>IAC-15.3: ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS</i>	89
<i>IAC-15.5: ACCOUNT MANAGEMENT RESTRICTIONS ON SHARED GROUPS/ACCOUNTS</i>	89
IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)	90
<i>IAC-16.1: PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED ACCOUNT INVENTORIES</i>	90
IAC-17: PERIODIC REVIEW OF ACCOUNT PRIVILEGES	91
IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT	91
IAC-19: CREDENTIAL SHARING	92
IAC-20: ACCESS ENFORCEMENT	92
<i>IAC-20.1: ACCESS ENFORCEMENT ACCESS TO SENSITIVE DATA</i>	92
<i>IAC-20.2: ACCESS ENFORCEMENT DATABASE ACCESS</i>	93
<i>IAC-20.3: ACCESS ENFORCEMENT USE OF PRIVILEGED UTILITY PROGRAMS</i>	93
IAC-21: LEAST PRIVILEGE	93
<i>IAC-21.3: LEAST PRIVILEGE PRIVILEGED ACCOUNTS</i>	94
IAC-22: ACCOUNT LOCKOUT	94
INCIDENT RESPONSE (IRO) POLICY & STANDARDS	95
IRO-01: INCIDENTS RESPONSE OPERATIONS	95
IRO-02: INCIDENT HANDLING	95
IRO-04: INCIDENT RESPONSE PROGRAM (IRP)	96
<i>IRO-04.1: INCIDENT RESPONSE PROGRAM (IRP) DATA BREACH</i>	96
IRO-05: INCIDENT RESPONSE TRAINING	97
IRO-06: INCIDENT RESPONSE TESTING	97
<i>IRO-06.1: INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS</i>	97
IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)	98
IRO-08: CHAIN OF CUSTODY & FORENSICS	98
IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS	98
IRO-10: INCIDENT STAKEHOLDER REPORTING	98
<i>IRO-10.3: INCIDENT STAKEHOLDER REPORTING VULNERABILITIES RELATED TO INCIDENTS</i>	99
<i>IRO-10.4: INCIDENT STAKEHOLDER REPORTING SUPPLY CHAIN COORDINATION</i>	99
IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	99
INFORMATION ASSURANCE (IAO) POLICY & STANDARDS	100
IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS	100
IAO-02: SECURITY ASSESSMENTS	100

IAO-02.2: SECURITY ASSESSMENTS SPECIALIZED ASSESSMENTS	100
IAO-04: THREAT ANALYSIS & FLAW REMEDIATION DURING DEVELOPMENT	101
MAINTENANCE (MNT) POLICY & STANDARDS	103
MNT-01: MAINTENANCE OPERATIONS	103
MNT-02: CONTROLLED MAINTENANCE	103
MNT-03: TIMELY MAINTENANCE	104
MOBILE DEVICE MANAGEMENT (MDM) POLICY & STANDARDS	105
MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES	105
MDM-02: ACCESS CONTROL FOR MOBILE DEVICES	105
MDM-05: REMOTE PURGING	106
NETWORK SECURITY (NET) POLICY & STANDARDS	107
NET-01: NETWORK SECURITY CONTROLS	107
NET-02: LAYERED DEFENSES	107
NET-03: BOUNDARY PROTECTION	107
NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)	108
NET-04.1: DATA FLOW ENFORCEMENT DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION	109
NET-06: NETWORK SEGMENTATION	110
NET-06.1: SECURITY FUNCTION ISOLATION SECURITY MANAGEMENT SUBNETS	110
NET-08: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)	110
NET-08.1: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS) DMZ NETWORKS	111
NET-13: ELECTRONIC MESSAGING	111
NET-14: REMOTE ACCESS	111
NET-14.5: REMOTE ACCESS WORK FROM ANYWHERE (WFA) – TELECOMMUTING SECURITY	112
NET-15: WIRELESS NETWORKING	112
NET-18: DNS & CONTENT FILTERING	113
PHYSICAL & ENVIRONMENTAL SECURITY (PES) POLICY & STANDARDS	114
PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS	114
PES-02: PHYSICAL ACCESS AUTHORIZATIONS	114
PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS ROLE-BASED PHYSICAL ACCESS	114
PES-03: PHYSICAL ACCESS CONTROL	115
PES-03.1: PHYSICAL ACCESS CONTROL CONTROLLED INGRESS & EGRESS POINTS	115
PES-03.3: PHYSICAL ACCESS CONTROL PHYSICAL ACCESS LOGS	116
PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES	116
PES-04.1: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES WORKING IN SECURE AREAS	117
PES-05: MONITORING PHYSICAL ACCESS	117
PES-05.1: MONITORING PHYSICAL ACCESS INTRUSION ALARMS/SURVEILLANCE EQUIPMENT	117
PES-05.2: MONITORING PHYSICAL ACCESS MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS	117
PES-06: VISITOR CONTROL	118
PES-07: SUPPORTING UTILITIES	118
PES-07.1: SUPPORTING UTILITIES AUTOMATIC VOLTAGE CONTROLS	118
PES-07.2: SUPPORTING UTILITIES EMERGENCY SHUTOFF	119
PES-07.3: SUPPORTING UTILITIES EMERGENCY POWER	119
PES-07.4: SUPPORTING UTILITIES EMERGENCY LIGHTING	119
PES-10: DELIVERY & REMOVAL	119
PES-12: EQUIPMENT SITING & PROTECTION	120
PES-12.1: EQUIPMENT SITING & PROTECTION TRANSMISSION MEDIUM SECURITY	120
PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS	121
PRIVACY (PRI) POLICY & STANDARDS	122
PRI-01: PRIVACY PROGRAM	122
PRI-01.3: PRIVACY PROGRAM DISSEMINATION OF PRIVACY PROGRAM INFORMATION	122
PRI-01.6: PRIVACY PROGRAM SECURITY OF PERSONAL DATA	122
PRI-02: PRIVACY NOTICE	122
PRI-02.1: PRIVACY NOTICE PURPOSE SPECIFICATION	123
PRI-03: CHOICE & CONSENT	123
PRI-04: RESTRICT COLLECTION TO IDENTIFIED PURPOSE	124
PRI-05: PERSONAL DATA RETENTION & DISPOSAL	124

<i>PRI-05.1: PERSONAL DATA RETENTION & DISPOSAL INTERNAL USE OF PERSONAL DATA FOR TESTING, TRAINING AND RESEARCH</i>	124
<i>PRI-05.3: PERSONAL DATA RETENTION & DISPOSAL DATA MASKING</i>	124
<i>PRI-05.4: PERSONAL DATA RETENTION & DISPOSAL USAGE RESTRICTIONS OF SENSITIVE PERSONAL DATA</i>	125
PRI-07: INFORMATION SHARING WITH THIRD PARTIES	125
<i>PRI-07.1: INFORMATION SHARING WITH THIRD PARTIES PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS</i>	125
PRI-08: TESTING, TRAINING & MONITORING	125
PROJECT & RESOURCE MANAGEMENT (PRM) POLICY & STANDARDS	127
PRM-01: SECURITY PORTFOLIO MANAGEMENT	127
PRM-02: SECURITY & PRIVACY RESOURCE MANAGEMENT	127
PRM-03: ALLOCATION OF RESOURCES	127
PRM-04: SECURITY & PRIVACY IN PROJECT MANAGEMENT	128
PRM-05: SECURITY & PRIVACY REQUIREMENTS DEFINITION	128
PRM-07: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT	128
RISK MANAGEMENT (RSK) POLICY & STANDARDS	129
RSK-01: RISK MANAGEMENT PROGRAM	129
<i>RSK-01.1: RISK MANAGEMENT PROGRAM (RMP) RISK FRAMING</i>	129
RSK-02: RISK-BASED SECURITY CATEGORIZATION	130
RSK-03: RISK IDENTIFICATION	130
RSK-04: RISK ASSESSMENT	130
<i>RSK-04.1: RISK ASSESSMENT RISK REGISTER</i>	131
RSK-05: RISK RANKING	131
RSK-06: RISK REMEDIATION	132
<i>RSK-06.1: RISK REMEDIATION RISK RESPONSE</i>	132
RSK-07: RISK ASSESSMENT UPDATE	132
RSK-08: BUSINESS IMPACT ANALYSIS (BIAs)	132
RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM	133
<i>RSK-09.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM SUPPLY CHAIN RISK ASSESSMENT</i>	134
RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)	134
SECURE ENGINEERING & ARCHITECTURE (SEA) POLICY & STANDARDS	135
SEA-01: SECURE ENGINEERING PRINCIPLES	135
<i>SEA-01.1: SECURE ENGINEERING PRINCIPLES CENTRALIZED MANAGEMENT OF CYBERSECURITY & PRIVACY CONTROLS</i>	136
SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE	136
<i>SEA-02.1: ALIGNMENT WITH ENTERPRISE ARCHITECTURE STANDARDIZED TERMINOLOGY</i>	136
SEA-17: SECURE LOG-ON PROCEDURES	136
SEA-20: CLOCK SYNCHRONIZATION	137
SECURITY OPERATIONS (OPS) POLICY & STANDARDS	138
OPS-01: OPERATIONS SECURITY	138
<i>OPS-01.1: OPERATIONS SECURITY STANDARDIZED OPERATING PROCEDURES (SOP)</i>	138
OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)	139
OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)	139
SECURITY AWARENESS & TRAINING (SAT) POLICY & STANDARDS	140
SAT-01: SECURITY & PRIVACY-MINDED WORKFORCE	140
SAT-02: SECURITY & PRIVACY AWARENESS	141
SAT-03: SECURITY & PRIVACY TRAINING	141
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) POLICY & STANDARDS	142
TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION	142
TDA-02: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS	142
<i>TDA-02.3: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS DEVELOPMENT METHODS, TECHNIQUES & PROCESSES</i>	142
TDA-05: DEVELOPER ARCHITECTURE & DESIGN	143
TDA-06: SECURE CODING	143
<i>TDA-06.1: SECURE CODING CRITICALITY ANALYSIS</i>	144
TDA-07: SECURE DEVELOPMENT ENVIRONMENTS	144
TDA-08: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS	145
TDA-09: SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT	145
TDA-10: USE OF LIVE DATA	146

TDA-14: DEVELOPER CONFIGURATION MANAGEMENT	146
TDA-15: DEVELOPER THREAT ANALYSIS & FLAW REMEDIATION	146
TDA-20: ACCESS TO PROGRAM SOURCE CODE	147
THIRD-PARTY MANAGEMENT (TPM) POLICY & STANDARDS	148
TPM-01: THIRD-PARTY MANAGEMENT	148
<i>TPM-01.1: THIRD-PARTY MANAGEMENT THIRD-PARTY INVENTORIES</i>	148
TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS	149
TPM-03: SUPPLY CHAIN PROTECTION	149
<i>TPM-03.1: SUPPLY CHAIN PROTECTION ACQUISITION STRATEGIES, TOOLS & METHODS</i>	149
<i>TPM-03.2: SUPPLY CHAIN PROTECTION LIMIT POTENTIAL HARM</i>	149
<i>TPM-03.3: SUPPLY CHAIN PROTECTION PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES</i>	150
TPM-04: THIRD-PARTY SERVICES	150
<i>TPM-04.1: THIRD-PARTY SERVICES THIRD-PARTY RISK ASSESSMENTS & APPROVALS</i>	150
<i>TPM-04.3: THIRD-PARTY SERVICES CONFLICT OF INTERESTS</i>	151
<i>TPM-04.4: THIRD-PARTY SERVICES THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS</i>	151
TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	151
<i>TPM-05.1: THIRD-PARTY CONTRACT REQUIREMENTS SECURITY COMPROMISE NOTIFICATION AGREEMENTS</i>	152
<i>TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX</i>	152
TPM-06: THIRD-PARTY PERSONNEL SECURITY	153
TPM-08: REVIEW OF THIRD-PARTY SERVICES	153
TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION	154
TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES	154
TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	154
THREAT MANAGEMENT (THR) POLICY & STANDARDS	155
THR-01: THREAT AWARENESS PROGRAM	155
THR-02: INDICATORS OF EXPOSURE (IOE)	155
THR-03: THREAT INTELLIGENCE FEEDS	155
VULNERABILITY & PATCH MANAGEMENT (VPM) POLICY & STANDARDS	157
VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	157
<i>VPM-01.1: VULNERABILITY & PATCH MANAGEMENT PROGRAM ATTACK SURFACE SCOPE</i>	157
VPM-02: VULNERABILITY REMEDIATION PROCESS	158
VPM-03: VULNERABILITY RANKING	158
VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES	158
<i>VPM-04.2: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES FLAW REMEDIATION WITH PERSONAL DATA (PD)</i>	159
VPM-05: SOFTWARE & FIRMWARE PATCHING	159
VPM-06: VULNERABILITY SCANNING	159
WEB SECURITY (WEB) POLICY & STANDARDS	161
WEB-02: USE OF DEMILITARIZED ZONES (DMZ)	161
GLOSSARY: ACRONYMS & DEFINITIONS	162
ACRONYMS	162
DEFINITIONS	162
KEY WORD INDEX	163
RECORD OF CHANGES	164
APPENDIX A – CROSSWALK MAPPING TO ISO 27001-27002 CONTROLS	165

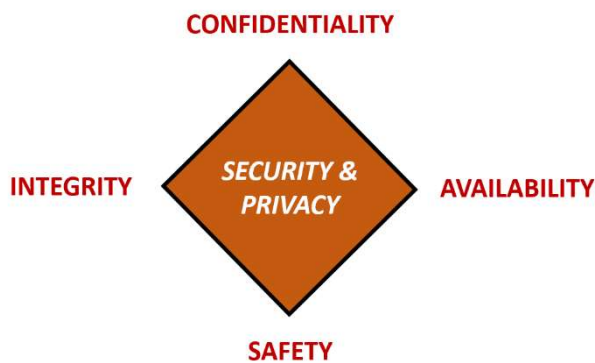
CYBERSECURITY AND DATA PROTECTION PROGRAM (CDPP) OVERVIEW

INTRODUCTION

The **Cybersecurity and Data Protection Program (CDPP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at ACME Professional Services, LLC (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 data and systems, applications and services. 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 privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services 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 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.

SECURE CONTROLS FRAMEWORK (SCF) STRUCTURE

The Cybersecurity & Data Protection Program (CDPP) leverages its structure and nomenclature from the Secure Controls Framework (SCF) to provide crosswalk mapping to:

- ISO 27001:2013
- ISO 27001:2022
- ISO 27002:2013
- ISO 27002:2013

The scope of the CDPP is tailored for ISO 27001 & 27002 controls, as shown in the crosswalk mapping in Appendix A at the back of this document.

PURPOSE

The purpose of the Cybersecurity and Data Protection Program (CDPP) is to prescribe a comprehensive framework for:

- Creating an Information Security Management System (ISMS) in accordance with ISO 27001.
- Protecting the confidentiality, integrity and availability of ACME data and information systems.
- Protecting ACME, its employees and its clients from illicit use of ACME information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support ACME's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Information Security risks.
- Providing for development, review and maintenance of minimum security controls required to protect ACME's data and information 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 users understand their day-to-day security responsibilities and the threats that could impact the company.

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.

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

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 regards 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 shall be effective immediately upon approval by management unless otherwise stated.

POLICY OVERVIEW

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

The CDPP 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 CDPP requirements.

ACME users 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.

MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION

The objective is to provide management direction and support for cybersecurity and data protection in accordance with business requirements and relevant laws and regulations.⁵

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind ACME's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with leading practices, ACME's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA) or Deming Cycle, approach:

- **Plan:** This phase involves designing the ISMS, assessing IT-related risks and selecting appropriate controls.
- **Do:** This phase involves implementing and operating the appropriate security controls.
- **Check:** This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- **Act:** This involves making changes, where necessary, to bring the ISMS back to optimal performance.

POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

ACME's cybersecurity and data protection documentation is comprised of five (5) core components:

- (1) **Policies** are established by the organization's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support the organization's overall strategy and mission;
- (2) **Control Objectives** identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
- (3) **Standards** provide organization-specific, quantifiable requirements for cybersecurity and data protection;
- (4) **Procedures** (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
- (5) **Guidelines** are additional guidance that is recommended, but not mandatory.

PROCEDURE

DEFINED PRACTICES / STEPS TO IMPLEMENT STANDARDS & GUIDELINES

GUIDELINE

ADDITIONAL, RECOMMENDED GUIDANCE THAT IS NOT MANDATORY

STANDARD

ORGANIZATION-SPECIFIC REQUIREMENTS TO SATISFY CONTROL OBJECTIVES

CONTROL OBJECTIVE

DESCRIBES WHAT IS TO BE ACHIEVED AS A RESULT OF IMPLEMENTING CONTROLS

POLICY

HIGH-LEVEL STATEMENT OF MANAGEMENT INTENT



Figure 1: Cybersecurity & Data Protection Documentation Structure

⁵ ISO 27002:2013 5.1

CYBERSECURITY & PRIVACY GOVERNANCE (GOV) POLICY & STANDARDS

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

Policy: 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. Cybersecurity and data protection controls shall be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and technology in use.

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

GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control Objective: The organization facilitates the implementation of cybersecurity and privacy governance controls.⁶

Standard: ACME's cybersecurity program 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 CDPP together provide complete coverage for all cybersecurity and privacy-related controls employed within the organization.

GOV-01.1: DIGITAL SECURITY GOVERNANCE PROGRAM | STEERING COMMITTEE

Control Objective: The organization coordinates cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.⁷

Standard: ACME must establish a cybersecurity and privacy steering committee, or advisory board, comprised of key stakeholders from ACME Lines of Business (LOB) and technology-related executives that:

- (a) Meets formally and on a regular basis; and
- (b) Receives briefings from the following:
 1. Chief Information Security Officer (CISO) on matters of cybersecurity;
 2. Chief Privacy Officer (CPO) on matters of privacy; and
 3. Chief Risk Officer (CRO) on matters of enterprise risk.

Guidelines: To achieve proper situational awareness across the organization, key cybersecurity and privacy leaders must facilitate communication with business stakeholders. This includes translating cybersecurity, privacy and risk concepts and language into business concepts and language as well as ensuring that business teams consult with cybersecurity and privacy teams to determine appropriate controls measures when planning new business projects.

The steering committee, or advisory board, can best advise the CISO, CPO and CRO on important matters pertaining to the organization to ensure technology, cybersecurity and privacy practices support the overall strategy and mission of the organization.

GOV-01.2: DIGITAL SECURITY GOVERNANCE PROGRAM | STATUS REPORTING TO GOVERNING BODY

Control Objective: The organization provides governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program.

Standard: ACME's Chief Information Security Officer (CISO) must:

- (a) Operate a repeatable process for reporting to ACME's board of directors, or similar oversight function; and

⁶ 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

⁷ ISO 27001-2013: 4.3, 6.2, 7.4, 9.3, 10.2

- (b) Provide detailed reporting, along with recommendations, to the oversight body; and
- (c) Document feedback received.

Guidelines: None

GOV-02: PUBLISHING CYBERSECURITY & PRIVACY DOCUMENTATION

Control Objective: The organization establishes, maintains and disseminates cybersecurity and privacy policies, standards and procedures.⁸

Standard: The Cybersecurity & Data Protection Program (CDPP) document represents the consolidation of ACME's cybersecurity and privacy policies and standards. The CDPP 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 CDPP, 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 and/or sensitive/regulated data.

Guidelines: An organization's cybersecurity policies create the roadmap for implementing cybersecurity and privacy measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. Without cybersecurity and privacy policies, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its statutory, regulatory and/or contractual obligations, nor being able to adequately protect its technology and data in a consistent manner.

GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY & PRIVACY PROGRAM

Control Objective: The organization reviews the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.⁹

Standard: ACME's business leadership (or other accountable business role or function) must review the Cybersecurity & Data Protection Program (CDPP) at planned intervals or as a result of changes to the organization (e.g., mergers, acquisitions, partnerships, new products, etc.) to ensure its continuing alignment with the security strategy, risk posture, effectiveness, accuracy, relevance and applicability to statutory, regulatory and/or contractual compliance obligations.

Guidelines: Updates to the CDPP 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.

GOV-04: ASSIGNED CYBERSECURITY & PRIVACY RESPONSIBILITIES

Control Objective: The organization assigns a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.¹⁰

Standard: Executive and line management must take formal action to support cybersecurity through clearly-documented direction and commitment and must ensure the action has been assigned. The overall authority and responsibility for managing the cybersecurity program are delegated to ACME's Chief Information Security Officer (CISO) and he/she must perform or delegate the following security management responsibilities:

- (a) Establish, document and distribute security policies and procedures;

⁸ 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: PM-1 | NIST CSF: ID.GV-1 | NIST SP 800-171A: 3.4.9[a], 3.9.2[a]

⁹ ISO 27001-2013: 6.1.1, 7.4 | ISO 27002-2022: 5.1, 5.37 | NIST SP 800-53 R5: PM-1

¹⁰ ISO 27001-2013: 5.3 | ISO 27002-2022: 5.2 | NIST SP 800-53 R5: PL-9, PM-2, PM-6, PM-29 | NIST CSF: ID.AM-6

CHANGE MANAGEMENT (CHG) POLICY & STANDARDS

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security 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.

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 on a production network.

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.⁴⁹

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 system, application and/or service must:

- (a) Be approved a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
- (b) Sufficiently document the following criteria to enable independent review:
 - 1. Reason for, and description of, the change;
 - 2. Documentation of security impact;
 - 3. Documented 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 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.

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.⁵⁰

⁴⁹ ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST CSF: PR.IP-3

⁵⁰ ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST CSF: PR.IP-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171A: 3.4.3[a], 3.4.3[b], 3.4.3[c], 3.4.3[d]

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 PANs) 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.⁵¹

Standard: Where technically feasible, data/process owners and asset custodians must test and validate configuration changes in a test environment, prior to deploying the change in the production environment.

Guidelines: When operating platforms are changed, mission-critical (SC1) and business-critical (SC2) technology assets 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.

⁵¹ 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)

THIRD-PARTY MANAGEMENT (TPM) POLICY & STANDARDS

Management Intent: The purpose of the Third-Party Management (TPM) policy is to ensure that cybersecurity and privacy risks associated with third-parties are minimized or avoided.

Policy: ACME shall implement and maintain industry-recognized Supply Chain Risk Management (SCRM) practices to strengthen the security and resilience of its third-party provider ecosystem. ACME's approach to SCRM requires transparency, so third-party provider inventories and risk assessments shall be generated to understand risks associated with dependencies, conflicts of interest, security practices and criticality considerations. As third-party providers' technology and processes evolve over time, ACME shall ensure the appropriate levels of due diligence and due care are applied to validate that necessary cybersecurity and privacy controls exist and are effective. Through sound procurement and contract management practices, ACME shall cultivate a secure third-party provider ecosystem that is conducive to security and resilience.

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

TPM-01: THIRD-PARTY MANAGEMENT

Control Objective: The organization facilitates the implementation of third-party management controls.³¹⁴

Standard: ACME must maintain a secure supply chain and requires:

- (a) Third-Party Service Providers (TSP) to be contractually bound to comply with ACME's applicable cybersecurity and privacy requirements; and
- (b) Data/process owners and asset custodians must maintain and implement procedures to manage TSP that includes, but is not limited to:
 1. Maintaining a list of service providers;
 2. Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of sensitive/regulated data the service providers possess or otherwise store, process or transmit on behalf of ACME or to the extent that they could impact the security of ACME;
 3. Ensures there is an established process for engaging service providers, including proper due diligence prior to engagement;
 4. Maintaining a program to monitor service providers' compliance status at least annually; and
 5. Maintaining information about which requirements are managed by each service provider and which are managed by ACME.

Guidelines: If the entity shares sensitive/regulated data with service providers (e.g., backup tape storage facilities, web hosting companies or security service providers), the process of due diligence should include:

- Direct observations;
- Reviews of policies and procedures; and
- Reviews of supporting documentation.

TPM-01.1: THIRD-PARTY MANAGEMENT | THIRD-PARTY INVENTORIES

Control Objective: The organization maintains a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.³¹⁵

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must develop and implement a third-party governance capability that maintains:

- (a) A current, accurate and complete list of ACME's Third-Party Service Providers (TSP);
- (b) A description for each of the services provided; and
- (c) The stakeholder(s) who are responsible for each TSP, on a contract basis.

Guidelines: Maintaining a list of all TSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface.

³¹⁴ ISO 27002-2022: 5.19, 5.20, 8.30 | NIST SP 800-53 R5: SA-4, SR-1 | NIST CSF: ID.BE-1, ID.SC-1 | NIST SP 800-171 R2: NFO - SA-4 | FAR: 52.204-21(c)

³¹⁵ ISO 27002-2022: 5.19

APPENDIX A – CROSSWALK MAPPING TO ISO 27001-27002 CONTROLS

The Cybersecurity & Data Protection Program (CDPP) leverages its structure and nomenclature from the Secure Controls Framework (SCF) to provide crosswalk mapping to:

- ISO 27001:2013
- ISO 27001:2022
- ISO 27002:2013
- ISO 27002:2013

The complete SCF is downloadable for free from <https://securecontrolsframework.com/> but this version of the CDPP only provides coverage for ISO 27001/27002 controls, as shown in the crosswalk mapping below:

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Cybersecurity & Privacy Governance	Digital Security Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.	GOV-01	4.3 4.4 5.1 6.1.1	4.4 5.1 5.1(a) 5.1(b) 5.1(c) 5.1(d) 5.1(e) 5.1(f) 5.1(g) 5.1(h) 6.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(c) 6.1.1(d) 6.1.1(e)(1) 6.1.1(e)(2) 8.1 10.1	5.1 5.1.1	5.1 5.4 5.37
Cybersecurity & Privacy Governance	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.	GOV-01.1	4.3 5.1 6.2 7.4 9.3 10.2	4.4 5.3 5.3(a) 5.3(b) 9.3 9.3.1 9.3.2(a) 9.3.2(b) 9.3.2(c) 9.3.2(d) 9.3.2(d)(1) 9.3.2(d)(2) 9.3.2(d)(3) 9.3.2(d)(4) 9.3.2(e) 9.3.2(f) 9.3.2(g) 9.3.3 10.1		
Cybersecurity & Privacy Governance	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program.	GOV-01.2		7.4 7.4(a) 7.4(b) 7.4(c) 7.4(d) 9.1 9.1(a) 9.1(b) 9.1(c) 9.1(d) 9.1(e)		

- SUPPLEMENTAL DOCUMENTATION -

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

ANNEXES, TEMPLATES & REFERENCES

Version 2023.2



INTERNAL USE

Access Limited to Internal Use Only

TABLE OF CONTENTS

ANNEXES	3
ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES	3
ANNEX 2: DATA CLASSIFICATION EXAMPLES	11
ANNEX 3: DATA RETENTION PERIODS	13
ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES	15
ANNEX 5: RULES OF BEHAVIOR (ACCEPTABLE & UNACCEPTABLE USE)	17
ANNEX 6: GUIDELINES FOR PERSONAL USE OF ORGANIZATIONAL IT RESOURCES	19
ANNEX 7: RISK MANAGEMENT FRAMEWORK (RMF)	20
ANNEX 8: SYSTEM HARDENING	23
ANNEX 9: SAFETY CONSIDERATIONS WITH EMBEDDED TECHNOLOGY	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
TEMPLATE 6: INCIDENT RESPONSE FORM	44
TEMPLATE 7: APPOINTMENT ORDERS (INFORMATION SECURITY OFFICER)	45
TEMPLATE 8: PRIVILEGED USER ACCOUNT REQUEST FORM	46
TEMPLATE 9: CHANGE MANAGEMENT REQUEST FORM	47
TEMPLATE 10: CHANGE CONTROL BOARD (CCB) MEETING MINUTES	49
TEMPLATE 11: RISK REGISTER	50
TEMPLATE 12: PORTS, PROTOCOLS & SERVICES (PPS)	51
TEMPLATE 13: BUSINESS IMPACT ANALYSIS (BIA)	52
TEMPLATE 14: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (BCP)	54
TEMPLATE 15: PRIVACY IMPACT ASSESSMENT (PIA)	58
REFERENCES	60
REFERENCE 1: CDPP EXCEPTION REQUEST PROCESS	60
REFERENCE 2: ELECTRONIC DISCOVERY (eDISCOVERY) GUIDELINES	61
REFERENCE 3: TYPES OF SECURITY CONTROLS	62
REFERENCE 4: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	63

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

Sensitive Personal Data (sPD)-Restricted

Personal Data (PD)-Restricted

Restricted

Confidential

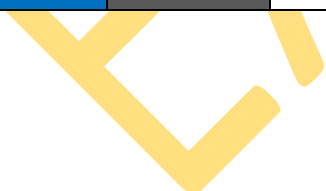
Internal Use

Public



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	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if CUI-Restricted information were to become available to unauthorized parties either internal or external to [Company Name]. · Impact could include negatively affecting [Company Name]’s competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company’s reputation.
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	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if sPD Restricted information were to become available to unauthorized parties either internal or external to [Company Name]. · Impact could include negatively affecting [Company Name]’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	<ul style="list-style-type: none"> · MODERATE DAMAGE would occur if PD Restricted information were to become available to unauthorized parties either internal or external to [Company Name]. · Impact could include negatively affecting [Company Name]’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	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to [Company Name]. · Impact could include negatively affecting [Company Name]’s competitive position, violating regulatory requirements, damaging the company’s reputation, violating contractual requirements and posing an identity theft risk.
Confidential	Definition	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally by [Company Name].
	Potential Impact of Loss	<ul style="list-style-type: none"> · MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name]. · Impact could include negatively affecting [Company Name]’s competitive position, damaging the company’s reputation and violating contractual requirements.
Internal Use	Definition	Internal Use information is information originated or owned by [Company Name] 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	<ul style="list-style-type: none"> · MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to [Company Name]. · 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	<ul style="list-style-type: none"> · NO DAMAGE would occur if Public information were to become available to parties either internal or external to [Company Name]. · Impact would not be damaging or a risk to business operations.



DATA HANDLING GUIDELINES

Note: For U.S. Government regulated data, the following requirements supersede [Company Name] data handling guidelines:

- For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handling:
 - 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 handling:
 - 32 CFR § 2002
 - DoD Instruction 5200.48
 - NIST SP 800-171 rev2

Handling Controls	CUI - RESTRICTED	SPD - RESTRICTED	PD - RESTRICTED	RESTRICTED	CONFIDENTIAL	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 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)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	No special requirements	No special requirements
External Network Transmission (wired & wireless)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication 	<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	Encryption is recommended	No special requirements

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	Confidential	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		
	First & Last Name					X		
Age					X			

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).

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

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 [Company Name].

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 [Company Name]'s ability to perform its mission;
- Public, wide-spread damage to [Company Name]'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 [Company Name]'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;
- Indirect revenue impact; and
- Indirect negative customer satisfaction.

Examples of SC3 systems, applications and services include, but are not limited to:

- *Test / Development / Staging environment*
- *Security Incident Event Monitor (SIEM) / log collector*
- *Internal / Intranet web functionality*

BUSINESS SUPPORTING (SC4)

Business Supporting (SC4) assets are the least important category of systems and handle information that is used in the conduct of routine, day-to-day business. SC4 systems are not mission-critical in the short or long term.

The impact of a SC4 system, or its data, being unavailable includes, but is not limited to:

- Localized employee productivity degradation;
- Localized delays or degradation of services or routine activities;
- No revenue impact; and
- No impact on customer satisfaction.

Examples of SC4 systems, applications and services include, but are not limited to:

- *Team-level metrics reporting*
- *Team-level productivity or reporting tools*

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the “level of effort” that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity						
		CUI - RESTRICTED	sPD - RESTRICTED	PD - RESTRICTED	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced
	SC2 Business Critical	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Basic	Basic
	SC3 Non-Critical	Enhanced	Enhanced	Basic	Enhanced	Basic	Basic	Basic
	SC4 Business Supporting	Enhanced	Enhanced	Basic	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

BASIC ASSURANCE REQUIREMENTS

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST SP 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

ENHANCED ASSURANCE REQUIREMENTS

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to [Company Name].