# I2 Documents - NIST 800-171 | CMMC Level 2

## i2 POLICY DOCUMENTS

1. Access Control Policy
2. Awareness and Training Policy
3. Audit and Accountability Policy
4. Configuration Management Policy
5. Identification and Authentication Policy
6. Incident Response Policy
7. Maintenance Procedure Policy
8. Media Protection Policy
9. Personnel Security Policy
10. Physical Protection Policy
11. Risk Assessment Policy
12. Security Assessment Policy
13. System and Communications Protection Policy
14. System and Information Integrity Policy
15. CUI Management Policy
16. Recovery Policy
17. Situational Awareness Policy
18. Acceptable Use Policy
19. Data Protection and CUI Security (Overarching Information Security) Policy
20. Acceptable Use for GCCH Email Policy
21. Personal Devise Use Policy

## I2 PROCEDURE DOCUMENTS

1. Backup and Recovery Procedure
2. Contractor Account Termination Procedure
3. IT Steering Group Meeting Procedure
4. External Information Connection Review Procedure
5. Inbrief | Outbrief Debrief Procedure
6. Media Protection Procedure
7. Physical Protection Procedure
8. Portable Storage Device Procedure
9. Posting to Public Media Procedure
10. Remote Access Procedure
11. Security Assessment Procedure
12. Situational Awareness Procedure
13. Software Approval Procedure
14. Termination and Offboarding Procedure
15. Visitor Procedure
16. Vulnerability Management Procedure
17. Configuration Documentation Revisions Procedure

18 Mobile Device Management Procedure
19 Training Procedure for Information Security
20 Asset Scan Procedure
21 Access and Authorization Matrix Procedure
22 Block External Domain Procedure
23 Maintenance Procedure
24 Unauthorized CUI Disclosure Procedure
25 Ransomware Procedure
26 Firewall Configuration, Segmentation, and Port Management Procedure
27 Security Alerts Procedure
28 Phish Mitigation Procedure
29 CUI Personnel Security Screening Procedure
30 Continuous Monitoring Procedure (Formerly: Audit and Logging)
31 Risk Management Procedure
32 Account Creation Procedure O365_GCCH
33 Endpoint Protection Procedure
34 Remote Access Desktop Support Procedure
35 System Security Architecture Design and System Engineering Procedure
36 Change Control Procedure
37 Wireless Network Access Procedure
38 Notice and Consent Procedure
39 Organizationally Defined Parameters (ODP) Procedure
40 Configuration Baseline Procedure
41 Nonessential Functionality Procedure
42 Alternative Worksite Procedure
43 FIPS Encryption Configuration Procedure
44 Onboarding Procedure
45 Intune Enrollment Procedure
46 Cisco Umbrella Procedure
47 Personal Device Use Procedure

## I2 PLANS, CATALOGS AND MATRICES

1 System Security Plan
2 Incident Response Plan
3 Configuration Management Plan
4 CUI Management Plan
5 Access & Authorization Matrix (AAM)
6 Document Traceability Matrix (DTM)
7 Configuration Baseline
8 Organizationally Defined Parameter Catalog
9 Risk Registry
10 MSSP/Customer Responsibility Matrix