#	CMMC Policy	Description
Domain 1: Access Control (AC)		
1	**Authorized Access Control Policy** Authorized Access Control [CUI Data] (AC.L2-3.1.1) *Level: 2*	The purpose of this policy is to ensure system access is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
2	**Transaction & Function Control Policy** Transaction & Function Control [CUI Data] (AC.L2-3.1.2) *Level: 2*	The purpose of this policy is to ensure system access is limited to the types of transactions and functions that authorized users are permitted to execute.
3	**Control CUI Flow Policy** Control CUI Flow (AC.L2-3.1.3) *Level: 2*	The purpose of this policy is to ensure the flow of CUI is controlled according to approved authorizations.
4	**Separation of Duties Policy** Separation of Duties (AC.L2-3.1.4) *Level: 2*	The purpose of this policy is to ensure the duties of individuals are separated to reduce the risk of malevolent activity without collusion.
5	**Least Privilege Policy** Least Privilege (AC.L2-3.1.5) *Level: 2*	The purpose of this policy is to ensure the organization employs the principle of least privilege, including specific security functions and privileged accounts.
6	**Non-Privileged Account Use Policy** Non-privilege Accounts Use (AC.L2-3.1.6) *Level: 2*	The purpose of this policy is to ensure that non-privileged accounts or roles are used when accessing non-security functions.
7	**Privileged Functions Policy** Privileged Functions (AC.L2-3.1.7) *Level: 2*	The purpose of this policy is to ensure the organization prevents non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
8	**Unsuccessful Logon Attempts Policy** Unsuccessful Logon Attempts (AC.L2-3.1.8) *Level: 2*	The purpose of this policy is to ensure unsuccessful logon attempts are limited.
9	**Privacy and Security Notices Policy** Privacy & Security Notices (AC.L2-3.1.9) *Level: 2*	The purpose of this policy is to ensure the organization provides privacy and security notices consistent with applicable CUI rules.
10	**Session Lock Policy** Session Lock (AC.L2-3.1.10) *Level: 2*	The purpose of this policy is to ensure the organization uses session locks with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

#	CMMC Policy	Description
11	**Session Termination Policy** Session Termination (AC.L2-3.1.11) *Level: 2*	The purpose of this policy is to ensure user sessions are terminated (automatically) after a defined condition.
12	**Control Remote Access Policy** Control Remote Access (AC.L2-3.1.12) *Level: 2*	The purpose of this policy is to ensure remote access sessions are monitored and controlled.
13	**Remote Access Confidentiality Policy** Remote Access Confidentiality (AC.L2-3.1.13) *Level: 2*	The purpose of this policy is to ensure cryptographic mechanisms are employed to protect the confidentiality of remote access sessions.
14	**Remote Access Routing Policy** Remote Access Routing (AC.L2-3.1.14) *Level: 2*	The purpose of this policy is to ensure remote access is routed via managed access control points.
15	**Privileged Remote Access Policy** Privileged Remote Access (AC.L2-3.1.15) *Level: 2*	The purpose of this policy is to ensure remote execution of privileged commands and remote access to security-relevant information is authorized.
16	**Wireless Access Authorization Policy** Wireless Access Authorization (AC.L2-3.1.16) *Level: 2*	The purpose of this policy is to ensure that wireless access is authorized before allowing such connections.
17	**Wireless Access Protection Policy** Wireless Access Protection (AC.L2-3.1.17) *Level: 2*	The purpose of this policy is to ensure the organization protects wireless access using authentication and encryption.
18	**Mobile Device Connection Policy** Mobile Device Connection (AC.L2-3.1.18) *Level: 2*	The purpose of this policy is to ensure the organization controls the connection of mobile devices.
19	**Encrypt CUI on Mobile Policy** Encrypt CUI on Mobile (AC.L2-3.1.19) *Level: 2*	The purpose of this policy is to ensure the organization encrypts CUI on mobile devices and mobile computing platforms.
20	**External Connections Policy** External Connections [CUI Data] (AC.L2-3.1.20) *Level: 2*	The purpose of this policy is to ensure the organization verifies and controls/limits connections to and use of external systems.
21	**Portable Storage Use Policy** Portable Storage Use (AC.L2-3.1.21) *Level: 2*	The purpose of this policy is to ensure the organization limits the use of portable storage devices on external systems.

#	CMMC Policy	Description
22	**Control Public Information Policy** Control Public Information [CUI Data] (AC.L2-3.1.22) *Level: 2*	The purpose of this policy is to ensure the CUI posted or processed on publicly accessible systems is controlled.
Domain 2: Awareness and Training (AT)		
23	**Role-Based Risk Awareness Policy** Role-Based Risk Awareness (AT.L2-3.2.1) *Level: 2*	The purpose of this policy is to ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
24	**Role-Based Training Policy** Role-Based Training (AT.L2-3.2.2) *Level: 2*	The purpose of this policy is to ensure personnel are trained to carry out their assigned information security-related duties and responsibilities.
25	**Insider Threat Awareness Policy** Insider Threat Awareness (AT.L2-3.2.3) *Level: 2*	The purpose of this policy is to ensure the organization provides security awareness training on recognizing and reporting potential indicators of insider threat.
Domain 3: Audit and Accountability (AU)		
26	**System Auditing Policy** System Auditing (AU.L2-3.3.1) *Level: 2*	The purpose of this policy is to ensure the organization creates and retains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
27	**User Accountability Policy** User Accountability (AU.L2-3.3.2) *Level: 2*	The purpose of this policy is to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
28	**Event Review Policy** Event Review (AU.L2-3.3.3) *Level: 2*	The purpose of this policy is to ensure the organization reviews, and updates logged events.
29	**Audit Failure Alerting Policy** Audit Failure Alerting (AU.L2-3.3.4) *Level: 2*	The purpose of this policy is to ensure the organization alerts in the event of an audit logging process failure.
30	**Audit Correlation Policy** Audit Correlation (AU.L2-3.3.5)	The purpose of this policy is to ensure the organization correlates audit record review,

#	CMMC Policy	Description
	Level: 2	analysis, and reporting processes for investigation and responds to indications of unlawful, unauthorized, suspicious, or unusual activity.
31	**Reduction & Reporting Policy** Reduction & Reporting (AU.L2-3.3.6) *Level: 2*	The purpose of this policy is to ensure the organization provides audit record reduction and report generation to support on-demand analysis and reporting.
32	**Authoritative Time Source Policy** Authoritative Time Source (AU.L2-3.3.7) *Level: 2*	The purpose of this policy is to ensure the organization provides a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
33	**Audit Protection Policy** Audit Protection (AU.L2-3.3.8) *Level: 2*	The purpose of this policy is to ensure the organization protects audit information and audit logging tools from unauthorized access, modification, and deletion.
34	**Audit Management Policy** Audit Management (AU.L2-3.3.9) *Level: 2*	The purpose of this policy is to ensure the organization limits the management of audit logging functionality to a subset of privileged users.
Domain 4: Configuration Management (CM)		
35	**System Baselining Policy** System Baselining (CM.L2-3.4.1) *Level: 2*	The purpose of this policy is to ensure the organization establishes and maintains baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
36	**Security Configuration Enforcement Policy** Security Configuration Enforcement (CM.L2-3.4.2) *Level: 2*	The purpose of this policy is to ensure the organization establishes and enforces security configuration settings for information technology products employed in organizational systems.
37	**System Change Management Policy** System Change Management (CM.L2-3.4.3) *Level: 2*	The purpose of this policy is to ensure the organization tracks, reviews, approves or disapproves, and logs changes to organizational systems.
38	**Security Impact Analysis Policy** Security Impact Analysis (CM.L2-3.4.4) *Level: 2*	The purpose of this policy is to ensure the organization analyzes the security impact of changes prior to implementation.

#	CMMC Policy	Description
39	**Access Restrictions for Change Policy** Access Restrictions for Change (CM.L2-3.4.5) *Level: 2*	The purpose of this policy is to ensure the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to organizational systems.
40	**Least Functionality Policy** Least Functionality (CM.L2-3.4.6) *Level: 2*	The purpose of this policy is to ensure the organization employs the principle of least functionality by configuring organizational systems to provide only essential capabilities.
41	**Nonessential Functionality Policy** Nonessential Functionality (CM.L2-3.4.7) *Level: 2*	The purpose of this policy is to ensure the organization restricts, disables, or prevents the use of nonessential programs, functions, ports, protocols, and services.
42	**Application Execution Policy** Application Execution Policy (CM.L2-3.4.8) *Level: 2*	The purpose of this policy addresses the deny-by-exception (blacklisting) policy to ensure the organization prevents the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
43	**User-Installed Software Policy** User-Installed Software (CM.L2-3.4.9) *Level: 2*	The purpose of this policy is to ensure the organization controls and monitors user-installed software.
Domain 5: Identification and Authentication (IA)		
44	**Identification Policy** Identification [CUI Data] (IA.L2-3.5.1) *Level: 2*	The purpose of this policy is to ensure the organization identifies system users, processes acting on behalf of users and devices.
45	**Authentication Policy** Authentication [CUI Data] (IA.L2-3.5.2) *Level: 2*	The purpose of this policy is to ensure the organization authenticates (or verifies) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
46	**Multifactor Authentication Policy** Multifactor Authentication (IA.L2-3.5.3) *Level: 2*	The purpose of this policy is to ensure the organization uses multifactor authentication for local and network access to privileged accounts and network access to non-privileged accounts.
47	**Replay-Resistant Authentication Policy** Replay-Resistant Authentication (IA.L2-3.5.4) *Level: 2*	The purpose of this policy is to ensure the organization employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

#	CMMC Policy	Description
48	**Identifier Reuse Policy** Identifier Reuse (IA.L2-3.5.5) *Level: 2*	The purpose of this policy is to ensure the organization prevents the reuse of identifiers for a defined period.
49	**Identifier Handling Policy** Identifier Handling (IA.L2-3.5.6) *Level: 2*	The purpose of this policy is to ensure the organization disables identifiers after a defined period of inactivity.
50	**Password Complexity Policy** Password Complexity (IA.L2-3.5.7) *Level: 2*	The purpose of this policy is to ensure the organization enforces minimum password complexity and change of characters when new passwords are created.
51	**Password Reuse Policy** Password Reuse (IA.L2-3.5.8) *Level: 2*	The purpose of this policy is to ensure the organization prohibits password reuse for a specified number of generations.
52	**Temporary Password Policy** Temporary Passwords (IA.L2-3.5.9) *Level: 2*	The purpose of this policy is to ensure the organization addresses temporary password use for system logons with an immediate change to a permanent password.
53	**Cryptographically-Protected Passwords Policy** Cryptographically-Protected Passwords (IA.L2-3.5.10) *Level: 2*	The purpose of this policy is to ensure the organization stores and transmits only cryptographically protected passwords.
54	**Obscure Feedback Policy** Obscure Feedback (IA.L2-3.5.11) *Level: 2*	The purpose of this policy is to ensure the organization obscures feedback on authentication information
Domain 6: Incident Response (IR)		
55	**Incident Handling Policy** Incident Handling (IR.L2-3.6.1) *Level: 2*	The purpose of this policy is to ensure the organization establishes an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
56	**Incident Reporting Policy** Incident Reporting (IR.L2-3.6.2) *Level: 2*	The purpose of this policy is to ensure the organization tracks, documents and reports incidents to designated officials and/or authorities both internal and external to the organization.
57	**Incident Response Testing Policy** Incident Response Testing (IR.L2-3.6.3)	The purpose of this policy is to ensure the organization tests the organizational incident

#	CMMC Policy	Description
	Level: 2	response capability.
Domain 7: Maintenance (MA)		
58	**Perform Maintenance Policy** Perform Maintenance (MA.L2-3.7.1) *Level: 2*	The purpose of this policy is to ensure the organization performs maintenance on organizational systems.
59	**System Maintenance Control Policy** System Maintenance Control (MA.L2-3.7.2) *Level: 2*	The purpose of this policy is to ensure the organization provides controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
60	**Equipment Sanitization Policy** Equipment Sanitization (MA.L2-3.7.3) *Level: 2*	The purpose of this policy is to ensure that the organization sanitizes any CUI from equipment removed for off-site maintenance.
61	**Media Inspection Policy** Media Inspection (MA.L2-3.7.4) *Level: 2*	The purpose of this policy is to ensure the organization checks media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
62	**Nonlocal Maintenance Policy** Nonlocal Maintenance (MA.L2-3.7.5) *Level: 2*	The purpose of this policy is to ensure the organization addresses multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminates such connections when nonlocal maintenance is complete.
63	**Maintenance Personnel Policy** Maintenance Personnel (MA.L2-3.7.6) *Level: 2*	The purpose of this policy is to ensure the organization supervises the maintenance activities of personnel without required access authorization.
Domain 8: Media Protection (MP)		
64	**Media Protection Policy** Media Protection (MP.L2-3.8.1) *Level: 2*	The purpose of this policy is to ensure the organization protects (i.e., physically controls and securely stores) system media containing CUI, both paper and digital.
65	**Media Access Policy** Media Access (MP.L2-3.8.2) *Level: 2*	The purpose of this policy is to ensure the organization limits access to CUI on system media to authorized users.
66	**Media Disposal Policy** Media Disposal [CUI Data] (MP.L2-3.8.3) *Level: 2*	The purpose of this policy is to ensure the sanitization or destruction of the system media containing CUI before disposal or release for

#	CMMC Policy	Description
		reuse is addressed.
67	**Media Markings Policy** Media Markings (MP.L2-3.8.4) *Level: 2*	The purpose of this policy is to ensure the organization marks media with necessary CUI markings and distribution limitations.
68	**Media Accountability Policy** Media Accountability (MP.L2-3.8.5) *Level: 2*	The purpose of this policy is to ensure the organization controls access to media containing CUI and maintains accountability for media during transport outside of controlled areas.
69	**Portable Storage Encryption Policy** Portable Storage Encryption (MP.L2-3.8.6) *Level: 2*	The purpose of this policy is to ensure the organization addresses the implementation of cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
70	**Removable Media Policy** Removable Media (MP.L2-3.8.7) *Level: 2*	The purpose of this policy is to ensure the organization controls the use of removable media on system components.
71	**Shared Media Policy** Shared Media (MP.L2-3.8.8) *Level: 2*	The purpose of this policy is to ensure the organization prohibits the use of portable storage devices when such devices have no identifiable owner.
72	**Protect Backups Policy** Protect Backups (MP.L2-3.8.9) *Level: 2*	The purpose of this policy is to ensure the organization protects the confidentiality of backup CUI at storage locations.
Domain 9: Personnel Security (PS)		
73	**Screen individuals Policy** Screen individuals (PS.L2-3.9.1) *Level: 2*	The purpose of this policy is to ensure the organization screens individuals prior to authorizing access to organizational systems containing CUI.
74	**Personnel Actions Policy** Personnel Actions (PS.L2-3.9.2) *Level: 2*	The purpose of this policy is to ensure that the organization protects its systems containing CUI during and after personnel actions, such as terminations and transfers.
Domain 10: Physical Protection (PE)		
75	**Limit Physical Access Policy** Limit Physical Access [CUI Data] (PE.L2-3.10.1)	The purpose of this policy is to ensure physical access to organizational systems, equipment, and the respective operating environments is limited to authorized individuals.

#	CMMC Policy	Description
	Level: 2	
76	**Monitor Facility Policy** Monitor Facility (PE.L2-3.10.2) *Level: 2*	The purpose of this policy is to ensure the organization protects and monitors the physical facility and supports infrastructure for organizational systems.
77	**Escort Visitors Policy** Escort Visitors [CUI Data] (PE.L2-3.10.3) *Level: 2*	The purpose of this policy is to ensure visitors are escorted and their activity is monitored.
78	**Physical Access Logs Policy** Physical Access Logs [CUI Data] (PE.L2-3.10.4) *Level: 2*	The purpose of this policy is to ensure the organization maintains audit logs of physical access.
79	**Manage Physical Access Policy** Manage Physical Access [CUI Data] (PE.L2-3.10.5) *Level: 2*	The purpose of this policy is to ensure the organization controls and manages physical access devices.
80	**Alternative Work Sites Policy** Alternative Work Sites (PE.L2-3.10.6) *Level: 2*	The purpose of this policy is to ensure the organization enforces safeguarding measures for CUI at alternate work sites.
Domain 11: Risk Assessment (RA)		
81	**Risk Assessments Policy** Risk Assessments (RA.L2-3.11.1) *Level: 2*	The purpose of this policy is to ensure the organization periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
82	**Vulnerability Scan Policy** Vulnerability Scan (RA.L2-3.11.2) *Level: 2*	The purpose of this policy is to ensure the organization scans for vulnerabilities in organizational systems and applications periodically, and when new vulnerabilities affecting those systems and applications are identified.
83	**Vulnerability Remediation Policy** Vulnerability Remediation (RA.L2-3.11.3) *Level: 2*	The purpose of this policy is to ensure the organization remediates vulnerabilities in accordance with risk assessments.

#	CMMC Policy	Description
Domain 12: Security Assessment (CA)		
84	**Security Control Assessment Policy** Security Control Assessment (CA.L2-3.12.1) *Level: 2*	The purpose of this policy is to ensure the organization periodically assesses the security controls in organizational systems to determine if the controls are effective in their application.
85	**Operational Plan of Action Policy** Operational Plan of Action (CA.L2-3.12.2) *Level: 2*	The purpose of this policy is to ensure the organization develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
86	**Security Control Monitoring Policy** Security Control Monitoring (CA.L2-3.12.3) *Level: 2*	The purpose of this policy is to ensure the organization monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls.
87	**System Security Plan Policy** System Security Plan (CA.L2-3.12.4) *Level: 2*	The purpose of this policy is to ensure the organization develops, documents and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
Domain 13: System and Communications Protection (SC)		
88	**Boundary Protection Policy** Boundary Protection [CUI Data] (SC.L2-3.13.1) *Level: 2*	The purpose of this policy is to ensure the organization monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the organizational systems.
89	**Security Engineering Policy** Security Engineering (SC.L2-3.13.2) *Level: 2*	The purpose of this policy is to ensure the organization employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
90	**Role Separation Policy** Role Separation (SC.L2-3.13.3) *Level: 2*	The purpose of this policy is to ensure the organization separates user functionality from system management functionality.
91	**Shared Resource Control Policy** Shared Resource Control (SC.L2-3.13.4)	The purpose of this policy is to ensure the organization prevents unauthorized and unintended information transfer via shared

#	CMMC Policy	Description
	Level: 2	system resources.
92	**Public-Access System Separation Policy** Public-Access System Separation [CUI Data] (SC.L2-3.13.5) *Level: 2*	The purpose of this policy is to ensure the implementation of subnetworks for publicly accessible system components that are physically or logically separated from internal networks is addressed.
93	**Network Communication by Exception Policy** Network Communication by Exception (SC.L2-3.13.6) *Level: 2*	The purpose of this policy is to ensure the organization denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
94	**Split Tunneling Policy** Split Tunneling (SC.L2-3.13.7) *Level: 2*	The purpose of this policy is to ensure the organization prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
95	**Data in Transit Policy** Data in Transit (SC.L2-3.13.8) *Level: 2*	The purpose of this policy is to ensure the organization implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
96	**Connections Termination Policy** Connections Termination (SC.L2-3.13.9) *Level: 2*	The purpose of this policy is to ensure the organization terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
97	**Key Management Policy** Key Management (SC.L2-3.13.10) *Level: 2*	The purpose of this policy is to ensure the organization establishes and manages cryptographic keys for cryptography employed in organizational systems.
98	**CUI Encryption Policy** CUI Encryption (SC.L2-3.13.11) *Level: 2*	The purpose of this policy is to ensure the organization employs FIPS-validated cryptography when used to protect the confidentiality of CUI.
99	**Collaborative Device Control Policy** Collaborative Device Control (SC.L2-3.13.12) *Level: 2*	The purpose of this policy is to ensure the organization prohibits remote activation of collaborative computing devices and provides an indication of devices in use to users present

#	CMMC Policy	Description
		at the device.
100	**Mobile Code Policy** Mobile Code (SC.L2-3.13.13) *Level: 2*	The purpose of this policy is to ensure the organization controls and monitors the use of mobile code.
101	**Voice over Internet Protocol Policy** Voice over Internet Protocol (SC.L2-3.13.14) *Level: 2*	The purpose of this policy is to ensure the organization controls and monitors the use of Voice over Internet Protocol (VoIP) technologies.
102	**Communications Authenticity Policy** Communications Authenticity (SC.L2-3.13.15) *Level: 2*	The purpose of this policy is to ensure the organization protects the authenticity of communication sessions.
103	**Protect CUI at Rest Policy** Data at Rest (SC.L2-3.13.16) *Level: 2*	The purpose of this policy is to ensure the organization protects the confidentiality of CUI at rest.
Domain 14: System and Information Integrity (SI)		
104	**Flaw Remediation Policy** Flaw Remediation [CUI Data] (SI.L2-3.14.1) *Level: 2*	The purpose of this policy is to ensure the organization identifies, reports, and corrects system flaws in a timely manner.
105	**Malicious Code Protection Policy** Malicious Code Protection [CUI Data] (SI.L2-3.14.2) *Level: 2*	The purpose of this policy is to ensure protection from malicious code is provided at designated locations within organizational systems.
106	**Security Alerts & Advisories Policy** Security Alerts & Advisories (SI.L2-3.14.3) *Level: 2*	The purpose of this policy is to ensure the organization monitors system security alerts and advisories and takes action in response.
107	**Update Malicious Code Protection Policy** Update Malicious Code Protection [CUI Data] (SI.L2-3.14.4) *Level: 2*	The purpose of this policy is to ensure malicious code protection mechanisms are updated when new releases are available.
108	**System & File Scanning Policy** System & File Scanning [CUI Data] (SI.L2-3.14.5) *Level: 2*	The purpose of this policy is to ensure the performance of periodic scans of the organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
109	**Monitor Communications for Attacks Policy**	The purpose of this policy is to ensure the organization monitors organizational systems,

#	CMMC Policy	Description
	Monitor Communications for Attacks (SI.L2-3.14.6) *Level: 2*	including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
110	**Identify Unauthorized Use Policy** Identify Unauthorized Use (SI.L2-3.14.7) *Level: 2*	The purpose of this policy is to ensure the organization identifies unauthorized use of organizational systems.
Conflict Resolution Policy		
111	**Conflict Resolution Policy**	The purpose of this policy is to ensure that every employee has the opportunity to raise issues and concerns regarding the workplace environment, interpersonal conflicts, or any misunderstandings, and to have these issues addressed promptly and with respect.