

TAQNYAT POLICY INDUSTRIAL INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

**ABSTRACT: TAQNYAT COMPANY POLICY FOR THE SAFETY, SECURITY, AND INTEGRITY OF
TAQNYAT COMPANY, EQUIPMENT, AND PERSONNEL, AND ASSURANCE OF BUSINESS
CONTINUITY IN THE EVENT OF SECURITY BREACHES OR ATTACKS**

AUTHOR CISO:YAZAN WALID ABDELRAHMAN

DOCUMENT VERSION 1 REVISION 90

FILENAME 1-TAQNYAT - IISMS-COMPANYPOLICY.DOCX

LAST MODIFICATION 1-FEB-2022 BY YAZAN ABDELRAHMAN

Contents

1.1.1	INTRODUCTION	3
1.2	NEED FOR A SECURITY POLICY	3
1.3	LEGAL REQUIREMENTS	4
1.4	WHO IS AFFECTED BY THE POLICY?	4
1.5	WHERE THE POLICY APPLIES.....	4
1.6	SECURITY POLICY OBJECTIVES.....	4
1.7	REVIEW AND AUDIT	5
1.7.1	RESPONSIBILITIES	6
1.8	RISK MANAGEMENT.....	6
1.9	AWARENESS	8
1.10	BUSINESS CONTINUITY/DISASTER RECOVERY.....	9
1.11	ASSET MANAGEMENT	9
1.12	PHYSICAL SECURITY	9
1.13	CLEAN DESK POLICY	10
1.14	SECURITY OF THIRD-PARTY ACCESS	11
1.15	COMPUTER USAGE	12
1.16	PASSWORD CONTROLS	13
1.17	DATA AND CONFIGURATION BACKUP	13
1.18	VIRUS / MALWARE	14
1.19	USER ACCESS CONTROL	14
1.20	ACCESS TO SYSTEMS	14
1.21	REGISTERING USERS.....	15
1.22	EMPLOYEES LEAVING	15
1.23	VISITORS AND CONTRACTORS	15

1.24	THE INTERNET	16
1.25	POWER SUPPLIES.....	16
1.26	NETWORK SECURITY	17
1.27	OPERATIONAL SECURITY	17
1.28	SYSTEM DOCUMENTATION	18
1.29	CONFIGURATION MANAGEMENT	19
1.30	MONITORING AND CONTINUOUS IMPROVEMENTS.....	19
1.31	SECURITY BREACH & INCIDENT MANAGEMENT.....	20

1.1.1 INTRODUCTION

TAQNYAT HIGH CONFIDENTIAL ARE STRIVE FOR THE HIGHEST LEVELS OF SAFETY AND SECURITY OF ALL INFORMATION TECHNOLOGY AND INDUSTRIAL AUTOMATION EQUIPMENT TO PREVENT OR MINIMIZE THE RISK OF PHYSICAL OR TECHNICAL HARM TO PERSONNEL, DAMAGE TO ANY DATA ASSETS OR LOSS OF INFORMATION, OR UNAUTHORIZED ACCESS AND/OR THEFT OR DESTRUCTION OF COMPANY DATA/INFORMATION.

1.2 NEED FOR A SECURITY POLICY

THIS INDUSTRIAL INFORMATION SECURITY MANAGEMENT SYSTEM (IISMS) POLICY DESCRIBES THE TAQNYAT HIGH CONFIDENTIAL REQUIREMENTS FOR MAINTAINING A SAFE AND SECURE ENVIRONMENT.

THIS IISMS IS MANDATED BY SECURITY ISCO AND TAQNYAT **MANAGEMENT**.

THE FREQUENCY OF CYBER-SECURITY RELATED ATTACKS ON FACTORIES IS INCREASING. THE IMPLEMENTATION OF APPROPRIATE SECURITY CONTROLS WILL HELP TO REDUCE OR ELIMINATE ANY RISKS TO THE SAFETY OF EMPLOYEES, OF EQUIPMENT, INFORMATION/DATA, AND THE BUSINESS ITSELF.

1.3 LEGAL REQUIREMENTS

TAQNYAT HIGH CONFIDENTIAL IS REQUIRED BY LAW TO COMPLY WITH THE FOLLOWING LOCAL, FEDERAL, OR INTERNATIONAL LAWS:

- NONE

1.4 WHO IS AFFECTED BY THE POLICY?

ALL EMPLOYEES, CONTRACTORS, AND VISITORS ARE REQUIRED TO ABIDE BY THIS IISMS POLICY, AND ALL RELATED POLICIES AND PROCEDURES.

1.5 WHERE THE POLICY APPLIES

THIS IISMS POLICY APPLIES TO ALL OF TAQNYAT DEPARTMENTS WHERE TAQNYAT HIGH CONFIDENTIAL IT DEPARTMENT HAVE THE FOLLOWING CONTROLS ARE APPROVED.

THIS POLICY COVERS:

- COMPUTER WORKSTATIONS, LAPTOPS, SERVERS, AND DISPLAY PANELS
- NETWORK EQUIPMENT, SWITCHES, ROUTERS, FIREWALLS, CABLING, AND WIRELESS COMMUNICATIONS
- PLCs AND ANY CONNECTED CONTROLLERS
- INDUSTRIAL EQUIPMENT
- SOFTWARE INSTALLED ON ANY COMPUTER SYSTEM

1.6 SECURITY POLICY OBJECTIVES

THE OBJECTIVES OF THIS SECURITY POLICY ARE:

- ASSURE THE PHYSICAL SAFETY OF ALL PERSONNEL, VISITORS, AND CONTRACTORS

- MAINTAIN CONFIDENTIALITY OF INFORMATION AND CONFIGURATION AND PREVENT INFORMATION DISCLOSURE TO UNAUTHORIZED PERSONNEL THROUGH DELIBERATE OR CARELESS ACTION
- PROTECT THE INTEGRITY OF INFORMATION TO PREVENT UNAUTHORIZED MODIFICATION OR DESTRUCTION OF INFORMATION OR CONFIGURATION
- ASSURE AVAILABILITY OF INFORMATION AND EQUIPMENT WHEN NEEDED
- MAINTAIN PRODUCTION QUALITY, QUANTITY, AND SAFETY
- COMPLY WITH LEGISLATIVE REGULATIONS (SEE LEGAL REQUIREMENTS ON PAGE 4)
- PREPARE, MAINTAIN, AND TEST BUSINESS CONTINUITY PLANS
- PROVIDE SECURITY TRAINING TO ALL EMPLOYEES, CONTRACTORS, AND VISITORS
- TO DETECT AND CONTAIN SECURITY BREACHES AS SOON AS POSSIBLE, ARE ESCALATED AND INVESTIGATED

1.7 REVIEW AND AUDIT

THIS POLICY AND ALL RELATED POLICIES AND PROCEDURES ARE REQUIRED TO:

- TWICE-YEARLY REVIEWS BY THE IT AND CYBER SECURITY ENGINEERS, LED BY THE PRINCIPAL ENGINEER, TO IDENTIFY AREAS OF WEAKNESS, TO DETERMINE ACCURACY, AND TO MAKE REVISIONS WHERE NECESSARY.
- ANNUAL REVIEWS BY IT DEPARTMENT CYBER-SECURITY TEAM TO PROVIDE SANITY CHECKING AND RECOMMENDATIONS
- REVIEW BY MANAGEMENT EVERY 2 YEARS.

IN ADDITION, THE FOLLOWING LIST OUTLINES AUDIT REQUIREMENTS:

- AN AUDIT CHECKLIST CONTAINS ALL TESTS AND VERIFICATIONS FOR TAQNYAT COMPANY INFRASTRUCTURE
- TWICE-YEARLY AUDIT OF ACTIVITIES CONDUCTED ON THE COMPANY TO ASSURE COMPLIANCE WITH ALL POLICIES
- AUDIT DOCUMENTATION TO DESCRIBE ALL FINDINGS
- NON-COMPLIANCES ARE IDENTIFIED AND ARE ESCALATED FOR REVIEW.

THIS I-ISMS MUST BE CONTINUALLY IMPROVED TO INCREASE SECURITY COVERAGE, DECREASE VULNERABILITIES, AND BE BETTER PREPARED TO HANDLE SECURITY BREACHES.

1.7.1 RESPONSIBILITIES

THE MANAGEMENT OF TAQNYAT HIGH CONFIDENTIAL CREATE AND REVIEW THIS POLICY.

MANAGEMENT WILL APPROVE THE POLICY AND SHOW PUBLIC SUPPORT BY OFFICIALLY ENDORSING THE IMMEDIATE IMPLEMENTATION AND ADOPTION.

THE PRINCIPAL ENGINEER OF THE INDUSTRIAL AUTOMATION DEPARTMENT FACILITATES THE IMPLEMENTATION IN ACCORDANCE WITH STANDARD OPERATING PROCEDURES AND IS THE PROJECT MANAGER AND ACTING CHIEF SECURITY OFFICER.

THE PRINCIPAL ENGINEER WILL FORM THE REQUIRED TEAMS TO FACILITATE THE IMPLEMENTATION AND ONGOING MAINTENANCE OF THIS I-ISMS.

ALL PERSONNEL, CONTRACTORS, AND VISITORS ARE REQUIRED TO REPORT SECURITY INCIDENTS OR TO NOTIFY OF ANY IDENTIFIED WEAKNESSES.

1.8 RISK MANAGEMENT

RISK MANAGEMENT IS THE PROCESS OF MAKING DECISIONS THAT WILL MINIMIZE OR ELIMINATE RISK TO THE SAFETY OF EMPLOYEES, EQUIPMENT, OR PROPERTY; TO PROTECT THE INVESTMENTS MADE IN INFRASTRUCTURE AND RESEARCH AND DEVELOPMENT; AND TO PROTECT BUSINESS INTERESTS.

A FORMAL PROCESS OF RISK IDENTIFICATION, REVIEW, AND MANAGEMENT IS REQUIRED WITH COMPLETE DOCUMENTATION WHICH MUST INCLUDE:

- RISK REGISTER CONTAINING ALL IDENTIFIED RISKS (NAME AND DESCRIPTION)
- CATEGORY OF RISK (PROCESS, MECHANICAL, CHEMICAL, INFORMATION, ETC.)
- LIKELIHOOD OF THE RISK OCCURRING (HIGH, MEDIUM, LOW)
- IMPACT ANALYSIS (INCLUDING UPSTREAM/DOWNSTREAM IMPACTS)
- ACTION (MITIGATE, TRANSFER, AVOID, ACCEPT)
- DECISION JUSTIFICATION

- DECISION MAKERS (CONTACTS)

THE RISK MANAGEMENT OBJECTIVES ARE TO:

- PREVENT THE REDUCTION OR ELIMINATION OF SAFETY FOR EMPLOYEES, EQUIPMENT, AND PROCESSES
- PREVENT THE EXPOSURE OF INDUSTRIAL AUTOMATION RESOURCES (INFRASTRUCTURE, CONTROLLERS, EQUIPMENT, PROCESSES, OR INFORMATION, ETC.) TO UNAUTHORIZED PERSONNEL AS WELL EXTERNAL ACTORS OUTSIDE OF THE COMPANY NETWORK (INTERNET, WI-FI, CORPORATE NETWORK, WAN, ETC.)
- PREVENT UNAUTHORIZED ACCESS/MODIFICATION/DESTRUCTION OF INDUSTRIAL AUTOMATION RESOURCES EQUIPMENT, INFORMATION, OR PROCESSES
- DETERMINE THE MOST COST-EFFECTIVE RESPONSE TO RISK THAT DOES NOT JEOPARDIZE SAFETY
- DEVELOP CONTINGENCY PLANS
- PREVENT FINANCIAL LOSSES DUE TO PRODUCTION LOSS, EQUIPMENT DAMAGE, PROCESS DISRUPTION, OR NON-COMPLIANCE TO REGULATIONS (SEE LEGAL REQUIREMENTS, ON PAGE 4)

THE FOLLOWING GUIDELINES APPLY TO THE RISK MANAGEMENT OF TAQNYAT HIGH CONFIDENTIAL AND MUST BE DOCUMENTED IN A RISK MANAGEMENT PLAN:

- AVOIDANCE:
 - DECREASED SAFETY OF PERSONNEL, EQUIPMENT, OR PROPERTY
 - EXPOSURE OF SYSTEMS, SERVICES, CONFIGURATION, OR INFORMATION TO UNAUTHORIZED PERSONS
 - VULNERABILITIES THAT CAN BE EXPLOITED IN EQUIPMENT, CONTROLLERS, COMPUTERS, SOFTWARE, OR INFRASTRUCTURE, THAT COULD BE EXPLOITED BY AN ATTACKER TO GAIN UNAUTHORIZED ACCESS, CONTROL, OR CONFIGURATION.
- MITIGATION:
 - POTENTIAL FOR DECREASED SAFETY OF PERSONNEL, EQUIPMENT, OR PROPERTY

- POTENTIAL EXPOSURE OF SYSTEM SERVICES OR INFORMATION TO UNAUTHORIZED PERSONS
 - DISRUPTION OF PRODUCTION
 - FINANCIAL LOSSES OR INCREASES TO BUSINESS EXPENSES
 - TRANSFERENCE:
 - WHERE THE COSTS FOR MITIGATION ARE TOO HIGH, BUT THE COSTS TO TRANSFER TO A THIRD PARTY (INSURANCE, CONTRACTOR, ETC.) ARE JUSTIFIABLE
 - INTERNAL RESOURCES ARE UNABLE TO MITIGATE (E.G. LACK OF SKILLS, LACK OF LABOR, ETC.)
 - ACCEPTANCE:
 - THERE IS NO WAY TO MITIGATE, TRANSFER, OR AVOID THE RISK, AND THE IDENTIFIED RISK ITEM/ASSET/PROCESS/RESOURCE/MATERIAL IS REQUIRED
 - THE COSTS FOR MITIGATION/TRANSFER ARE TOO HIGH, BUT THE IMPACT IS NEGLIGIBLE IF THE RISK TRANSPIRES
-

1.9 AWARENESS

CYBER-SECURITY ESSENTIAL AND REQUIRES THE PARTICIPATION OF ALL PERSONNEL, AND MUST COVER BY MINIMUM:

- AWARENESS AND TRAINING ARE REQUIRED FOR ALL PERSONNEL ON THE EXISTENCE OF THIS I-ISMS POLICY
- HOW TO CONDUCT THEIR WORK SAFELY
- HOW TO IDENTIFY SOCIAL ENGINEERING ATTACKS (EMAIL, PHONE, IN-PERSON)
- IDENTIFYING TELL-TALE SIGNS OF A BREACH, HOW TO RESPOND, AND WHO TO NOTIFY AND WHEN

AWARENESS TRAINING ARE ACHIEVED BY CONTRACTING A CYBER SECURITY SPECIALIST AND TRAINER IN ORDER TO:

- CONTINUALLY EVOLVE AND IMPROVE AS NEEDED
- OCCUR IMMEDIATELY FOR NEW EMPLOYEES, CONTRACTORS, AND VISITORS

- OCCUR ANNUALLY FOR ALL ENGINEERS AND TAQNYAT WORKERS

1.10 BUSINESS CONTINUITY/DISASTER RECOVERY

THE BUSINESS CONTINUITY (BC) / DISASTER RECOVERY (DR) POLICY IS TO ENSURE ALL TAQNYAT PROCESSES CAN BE KEPT AT NORMAL OR NEAR-NORMAL PERFORMANCE FOLLOWING AN INCIDENT THAT HAS THE POTENTIAL TO SIGNIFICANTLY HARM THE VIABILITY OF TAQNYAT HIGH CONFIDENTIAL AS FOLLOWS:

- THE INDUSTRIAL AUTOMATION DEPARTMENT OF TAQNYAT HIGH CONFIDENTIAL ARE RESPONSIBLE FOR THE CREATION, REVIEW AND APPROVAL, TESTING, AND CONTINUOUS EVOLVEMENT OF THE BC/DR PLAN.
- BC/DR MUST BE REVIEWED ANNUALLY
- BC/DR MUST BE TESTED AT LEAST ONCE ANNUALLY

1.11 ASSET MANAGEMENT

ALL INDUSTRIAL AUTOMATION EQUIPMENT, INFRASTRUCTURE, COMPUTERS, DEVICES, PERIPHERALS, AND SOFTWARE MUST BE LOGGED IN AN AN ASSET REGISTER TO:

- IDENTIFY ALL ASSETS AND CATEGORIZE (CRITICAL, IMPORTANT, NEUTRAL, NEGLIGIBLE, ETC.)
- COMPLEMENT THE RISK REGISTER (SEE RISK MANAGEMENT, ON PAGE 6)
- CATALOG ALL EQUIPMENT (NETWORK INFRASTRUCTURE, COMPUTERS, SERVERS, INDUSTRIAL EQUIPMENT, CONTROLLERS, ETC.)
- CATALOG ALL SOFTWARE SYSTEMS AND COMPONENTS

FREQUENT REVIEW AND MAINTENANCE OF THE EQUIPMENT REGISTER IS REQUIRED.

1.12 PHYSICAL SECURITY

TAQNYAT HIGH CONFIDENTIAL COMPANY CONTAINS EQUIPMENT THAT WELL PHYSICAL SECURED BY FOLLOWING AND APPLIES TO THE COMPANY:

- ACCESS DOORS INTO THE PRODUCTION AREA IS REMAIN LOCKED AT ALL TIMES TO PREVENT UNAUTHORIZED ACCESS
- OTHER ACCESS METHODS (WINDOWS, VENTS, FIRE-ESCAPE, ETC.) TO THE PRODUCTION AREA IS ALSO PROTECTED IN ORDER TO PREVENT UNAUTHORIZED ACCESS

OFFICE SPACE WITHIN THE TAQNYAT COMPANY MUST BE SECURED AS FOLLOWS:

- LOCKABLE DOOR, TO ALWAYS REMAIN LOCKED
- LOCKABLE FILING SYSTEMS / STORAGE
- NO SENSITIVE INFORMATION IS VISIBLE OR EASILY ACCESSIBLE (SEE CLEAN DESK POLICY BELOW)

THE FOLLOWING APPLIES TO THE HEAVY EQUIPMENT, DEVICES, CONTROLLERS, AND COMPUTERS, ETC.:

- SUITABLY ANCHORED TO A STRONG SURFACE TO PREVENT THEFT OR MOVEMENT, ETC.
- SUITABLY OBSTRUCTED TO PREVENT UNAUTHORIZED ACCESS (E.G. BEHIND DOOR OR SECURE ACCESS PANEL, IN A LOCKABLE CAGE/RACK, ETC.)

1.13 CLEAN DESK POLICY

SENSITIVE INFORMATION SUCH AS LOGIN CREDENTIALS, INSTRUCTIONS, OR SENSITIVE/CONFIDENTIAL INFORMATION ETC., IS AVAILABLE TO AUTHORIZED PERSONNEL ONLY. THEREFORE, THE CLEAN-DESK POLICY EXISTS AS FOLLOWS:

- SENSITIVE INFORMATION MUST NOT BE LEFT IN A VISIBLE AND/OR ACCESSIBLE LOCATION SUCH AS A DESK, MONITOR, OR WALL, ETC.
- SENSITIVE INFORMATION IS MOVED TO A SECURE LOCATION (FILING CABINET, LOCKABLE DRAWER, ETC.) WHEN NOT BEING ACTIVELY USED, OR WHEN THE EMPLOYEE MUST LEAVE THE LOCATION.
- COMPUTERS AND OPERATOR DISPLAY MUST ARE OFF OR LOCKED OR LOGGED-OUT WHEN NOT IN USE, OR IF AN EMPLOYEE MUST TEMPORARILY LEAVE THEIR STATION.

- DESKS, DRAWERS, CABINETS, CLOSETS, AND OTHER STORAGE MEDIUM MUST REMAIN LOCKED WHEN NOT IN USE.
- SENSITIVE INFORMATION THAT IS NO LONGER NEEDED MUST BE DISPOSED OF VIA A DOCUMENT SHREDDER.
- OTHER WRITING INSTRUMENTS SUCH AS WHITEBOARDS, BLACKBOARDS, FLIPCHARTS, OR ELECTRONIC DISPLAYS THAT CONTAIN SENSITIVE INFORMATION MUST BE ERASED/CLEANED/SHREDDED AS APPROPRIATE.
- ANY PORTABLE MEDIA (CDROM, DVD, BLU-RAY, USB STICK, MEMORY CARDS, EXTERNAL DRIVES, ETC.) THAT CONTAINS SENSITIVE INFORMATION MUST BE LOCKED-AWAY OR PROPERLY DISPOSED OF (DESTROYED) AS APPROPRIATE.

1.14 SECURITY OF THIRD-PARTY ACCESS

THE FOLLOWING LIST APPLIES TO EXTERNAL PARTIES (CONTRACTORS/VISITORS) THAT REQUIRE ACCESS TO **TAQNYAT HIGH CONFIDENTIAL** ASSETS:

- THEY ARE SIGN-IN TO A VISITOR'S LOG
- THEY MUST BOUND TO THE INFORMATION SECURITY POLICIES OF **TAQNYAT HIGH CONFIDENTIAL**
- ACCESS TO SECURE AREAS AND CRITICAL ASSETS ALWAYS REQUIRES SUPERVISION
- ACCESS TO CONTROLLERS, COMPUTERS, AND SERVERS REQUIRES EITHER:
 - SUPERVISION ALWAYS, OR RESTRICTED ACCESS THAT WILL LIMIT ACCESS/CAPABILITIES AND NOT NECESSITATE THE NEED FOR SUPERVISION

THE FOLLOWING LIST APPLIES TO EXTERNAL PARTIES (SERVICE-PROVIDERS) THAT REQUIRE ACCESS TO INFRASTRUCTURE SUCH AS THE NETWORK, SCADA, OR EQUIPMENT/DEVICES FOR MONITORING PURPOSES:

- THEY MUST BOUND TO THE SECURITY POLICIES OF **TAQNYAT HIGH CONFIDENTIAL**
- AN APPROPRIATE AGREEMENT (SERVICE LEVEL AGREEMENT) IS SIGNED BY MANAGEMENT (ANAS) EXISTS

A DOCUMENTATION TRAIL OF ALL THIRD-PARTY ACCESS, CONTACT INFORMATION, AND SUMMARY OF ACTIVITIES ARE AVAILABLE UPON REQUEST.

1.15 COMPUTER USAGE

COMPUTER SYSTEMS ARE PROVIDED FOR EMPLOYEES TO CONDUCT THEIR WORK IN ACCORDANCE WITH THE FOLLOWING RULES:

- TAQNYAT COMPUTER SYSTEMS ARE COMPANY PROPERTY AND FOR COMPANY USE ONLY
- EMPLOYEES ADHERE TO ALL COMPANY POLICIES INCLUDING ACCEPTABLE USE ETC.
- SOFTWARE INSTALLATION IS PROHIBITED, EXCEPT WHEN THE SOFTWARE IS FOR OFFICIAL COMPANY USE ONLY.
- STORAGE OF PERSONAL INFORMATION/DATA IS PROHIBITED
- INTERNET USE IS PERMITTED ON DESIGNATED WORKSTATIONS ONLY AND IS NOT PERMITTED ON ANY COMPUTER HOSTING SCADA SYSTEMS OR MONITORING/CONTROLLING COMPANY EQUIPMENT OR PROCESSES
- TAQNYAT IS RESTRICT ANY REMOVAL OR DEACTIVATION OF ANY SECURITY CONTROLS, SOFTWARE SYSTEMS, OR DATA, IS NOT PERMITTED

TAQNYAT COMPUTER SYSTEMS IS SECURED AS FOLLOWS:

- PREVENT UNAUTHORIZED PHYSICAL ACCESS
- PREVENT UNAUTHORIZED REMOTE ACCESS
- PREVENT INTERNET ACCESS DURING NORMAL OPERATIONS
- ENABLE MONITORING OF KEY SYSTEM FILES TO DETECT CHANGES
- CONTAIN A SUITABLY CONFIGURED FIREWALL
- PREVENT THE AUTOMATIC UPDATE OF O/S AND APPLICATION PATCHES/UPDATES
- ENABLE AUDIT LOGGING OF USER/SYSTEM ACTIVITIES
- HARDEN THE O/S AND APPLICATIONS TO REMOVE UNNECESSARY/UNUSED COMPONENTS, SERVICES, APPLICATIONS, AND INTERFACES, ETC.

ALL OTHER COMPUTER SYSTEMS SUCH AS WORKSTATIONS, SERVERS, AND LAPTOPS ETC. IS ALSO SECURED AS DEFINED IN THE PREVIOUS LIST FOR TAQNYAT COMPUTERS, BUT WITH THE FOLLOWING EXCEPTIONS:

- OPERATING SYSTEM AND APPLICATIONS ARE CONFIGURED TO AUTOMATICALLY UPDATE WITH THE LATEST PATCHES AND SERVICE PACKS
- ANTI-VIRUS AND ANTI-MALWARE COMPONENTS ARE CONFIGURED TO AUTOMATICALLY UPDATE SIGNATURES

1.16 PASSWORD CONTROLS

PASSWORDS MUST BE IMPLEMENTED WHERE POSSIBLE, FOR COMPUTERS, SOFTWARE, NETWORK INFRASTRUCTURE, AND DEVICES ETC. AND MUST ABIDE BY THESE RULES:

- ALL USERS HAVE THEIR OWN UNIQUE LOGIN PASSWORD
- PASSWORDS ARE COMPLEX:
 - A MINIMUM OF 7 CHARACTERS
 - IT IS CONTAINED UPPER CASE AND LOWER-CASE CHARACTERS
 - IT IS CONTAIN A NUMBER AND SPECIAL CHARACTER
- THE PASSWORDS ARE CHANGED FREQUENTLY; THE INTERVAL MAY VARY FROM SYSTEM TO SYSTEM AS APPROPRIATE

1.17 DATA AND CONFIGURATION BACKUP

ALL COMPANY INFORMATION/DATA AND CONFIGURATION SETTINGS ARE BACKED-UP AS IT MAY BE REQUIRED FOR RESTORATION IN THE EVENT OF DESTRUCTION OR EQUIPMENT FAILURE, AS FOLLOWS:

- MACHINE CONFIGURATION SETTINGS ARE EXPORTED TO FILE FOR SECURE BACKUP; IF THIS IS NOT POSSIBLE, THEN ALL SETTINGS MUST BE DOCUMENTED INSTEAD
- PLC/CONTROLLER SETTINGS AND LADDER-LOGIC (PROGRAMMING) CODE ARE EXPORTED TO OFFLINE FILE
- COMPUTER SYSTEMS COMPLETE BACKUP OF OPERATING SYSTEM AND DATA ARE BACKED-UP

- MANUAL BACKUPS ARE SCHEDULED AND UNDER THE RESPONSIBILITY OF ISCO AND IT MANAGER TO ASSURE THE WORK IS DONE.
 - BACKUP MEDIA (DISKS, CD/DVD/BLU-RAY, MEMORY-STICKS, TAPE, ETC.) IS SECURED BY USING PASSWORD-BASED ENCRYPTION
-

1.18 VIRUS / MALWARE

ALL COMPUTER SYSTEMS HAVE THE FOLLOWING FEATURES:

- CONTAIN ADEQUATE AND UP-TO-DATE ANTI-VIRUS AND ANTI-MALWARE
 - MUST BE CONFIGURED TO:
 - AUTOMATICALLY UPDATE ANTI-VIRUS SIGNATURES IS ENABLED.
 - REAL-TIME SCANNING IS ENABLED
 - THEY ARE SET TO BE AUTOMATICALLY SCAN THE WHOLE COMPUTER SYSTEM AT LEAST WEEKLY
 - DEACTIVATION OF ANTI-VIRUS IS PROHIBITED
-

1.19 USER ACCESS CONTROL

ALL **DEPARTMENT**S EMPLOYEES NEED ACCESS TO COMPUTER EQUIPMENT AND/OR INDUSTRIAL EQUIPMENT AND ARE THEREFORE SUBJECT TO THE POLICIES CONTAIN IN THE FOLLOWING SUB-SECTIONS.

1.20 ACCESS TO SYSTEMS

A POLICY OF LEAST-PRIVILEGE IS ENFORCED FOR ALL LOCATIONS, COMPUTER SYSTEMS, APPLICATIONS, AND DEVICES/MACHINES ETC.:

- PHYSICAL SYSTEMS:
 - TAQNYAT ENSURE THAT THE KEYS TO DOORS, DRAWERS, CABINETS, CAGES, OR CLOSETS, ETC. ARE THE RESPONSIBILITY OF MANAGERS AND REMAIN IN THE POSSESSION OF MANAGERS AND SECURITY GUARDS ONLY

- ELECTRONIC SYSTEMS:
 - USERS THAT NEED ACCESS SHALL BE GRANTED ACCESS, ONLY
 - USERS THAT ARE GRANTED ACCESS MUST RECEIVE THE CAPABILITIES THEY NEED ONLY
-

1.21 REGISTERING USERS

THE MODIFICATION OF SYSTEMS TO ADJUST ACCESS MUST BE CONTINUOUS AND BASED ON A REVIEW OF THE APPROPRIATE MANAGER/MANAGEMENT AS FOLLOWS:

- ANY NEW ADDITION OF NEW USERS IT MUST BE APPROVED BY A MANAGER WITH CLEAR DIRECTION ON THE CAPABILITIES NEEDED BY THE USER
 - THE MODIFICATION OF EXISTING USERS MUST BE APPROVED BY A MANAGER
 - THE REMOVAL OF EXISTING USERS MUST BE APPROVED BY A MANAGER
-

1.22 EMPLOYEES LEAVING

THIS POLICY REQUIRES THE FOLLOWING WHENEVER AN EMPLOYEE RESIGN FROM **TAQNYAT HIGH CONFIDENTIAL**:

- KEYS TO DOORS, CAGES, CABINETS, DRAWERS, ETC. ARE RETRIEVED
 - INFORMATION AND CONFIDENTIAL INFORMATION THAT IS IN PRINT, OR STORED ON MEDIUM SUCH AS CD/DVD, USB, ONLINE STORAGE ETC. ARE RETURNED TO TAQNYAT.
 - ACCESS TO COMPUTER SYSTEMS WILL BE REMOVED
 - ACCESS TO INDUSTRIAL EQUIPMENT WILL BE REMOVED
 - ACCESS TO SENSITIVE/CONFIDENTIAL INFORMATION WILL BE REMOVED
-

1.23 VISITORS AND CONTRACTORS

TAQNYAT FOLLOWING ENFORCED IN ORDER TO PROTECT COMPANY ASSETS, PROCESSES, CONFIGURATION SETTINGS, AND CONFIDENTIAL INFORMATION:

- ADMINISTRATIVE ACCESS TO ANY DEVICE, COMPUTER, OR SYSTEM ETC., IS PROHIBITED UNLESS CONSTANT SUPERVISION FROM **TAQNYAT HIGH CONFIDENTIAL** EMPLOYEE(S) IS AVAILABLE.
- IF VISITOR REQUIRES ACCESS TO A DEVICE OR COMPUTER SYSTEM FOR EXTENDED PERIODS OF TIME, THEN A TEMPORARY ACCOUNT SHOULD BE CREATED AND USED THAT IS:
 - LIMITED IN CAPABILITIES
 - EXPIRES AT A SPECIFIC DATE/TIME

1.24 THE INTERNET

INTERNET ACCESS HAS THE POTENTIAL TO COMPLETELY DISRUPT BUSINESS OPERATIONS.

THEREFORE, ALL PERSONS ACCESSING THE INTERNET DO SO WITHIN THE SCOPE AND BOUNDARIES OF ALL **TAQNYAT HIGH CONFIDENTIAL** POLICIES.

- INTERNET ACCESS FROM TAQNYAT COMPUTERS IS STRICTLY PROHIBITED
- INTERNET ACCESS IS PERMITTED ON DESIGNATED COMPUTERS ONLY
- USE OF AN APPROVED BROWSER WITH AN APPROVED CONFIGURATION ONLY
- USE OF AN APPROVED EMAIL CLIENT WITH APPROVED CLIENT CONFIGURATION ONLY
- ALL ACTIVITY IS LOGGED
- THE REMOVAL OF BROWSING HISTORY AND CACHE IS NOT PERMITTED

1.25 POWER SUPPLIES

THE POWER TO EQUIPMENT MAY VARY FROM SMALL ELECTRONICS UTILIZING MAMPS THERE IS NO ANY HEAVY EQUIPMENT USING MORE THAN 220V OR MORE. POWER SUPPLY IS ESSENTIAL AND THEREFORE:

- ALL POWER-OUTLETS ARE SECURED FOR AUTHORIZED PERSONNEL ONLY
- ALL POWER-CONNECTORS TO DEVICES ARE SECURED FOR AUTHORIZED PERSONNEL ONLY

- ALL POWER CABLES ARE ANCHORED TO STABLE SURFACES TO ELIMINATE ANY MOVEMENT
- ALL POWER CABLES ARE SHIELDED TO PREVENT DAMAGE OR DISRUPTION
- ALL POWER ADAPTERS, CABLES, AND PLUGS ARE CATALOGED IN THE ASSET REGISTER

1.26 NETWORK SECURITY

THE COMMUNICATIONS PLATFORM REQUIRED BY TAQNYAT COMPUTER SYSTEMS, CONTROLLERS/PLCs, AND MACHINES/DEVICES ETC., ARE SECURED AS FOLLOWS:

- NETWORK INFRASTRUCTURE COMPONENTS (ROUTERS, SWITCHES, FIREWALLS, ETC.) ARE ACCESSIBLE TO AUTHORIZED PERSONNEL ONLY, IS SUFFICIENTLY HARDENED TO REDUCE ATTACK SURFACES, AND IS PHYSICALLY PROTECTED IN A SAFE LOCATION (ROOM OR RACK, ETC.)
- NETWORK CABLING IS SECURED FROM ACCIDENTAL DAMAGE
- NETWORK ACCESS IS RESTRICTED TO AUTHORIZED USERS ONLY, AND AUTHORIZED EQUIPMENT ONLY
- NETWORK COMMUNICATIONS (PROTOCOLS) ARE LIMITED TO AUTHORIZED APPLICATIONS AND SYSTEMS ONLY, AND INTER-DEVICE COMMUNICATIONS ARE CONTROLLED
- EXTERNAL NETWORK ACCESS, IF REQUIRED, IS HIGHLY RESTRICTIVE AND LIMITED TO AUTHORIZED PERSONNEL AND SYSTEM ADMINS ONLY
- ALL NETWORK ACTIVITIES ARE LOGGED

1.27 OPERATIONAL SECURITY

THE SUCCESSFUL OPERATIONS OF PRODUCTION ARE DEPENDENT ON NUMEROUS SYSTEMS WHICH IS SECURED AS FOLLOWS:

- NETWORK INFRASTRUCTURE (SEE NETWORK SECURITY, ON PAGE 17) AND COMPUTER SYSTEMS (SEE PHYSICAL SECURITY, ON PAGE 9 AND COMPUTER USAGE, ON PAGE 12) ARE ADEQUATELY SECURED FROM UNAUTHORIZED ACCESS OR RE-CONFIGURATION
- DEVICE/MACHINE/EQUIPMENT ACCESS AND CONFIGURATION IS SECURED (SEE USER ACCESS CONTROL, ON PAGE 14)
- DEVICE CONFIGURATION IS DOCUMENTED (SEE SYSTEM DOCUMENTATION, BELOW)
- DEVICE CONFIGURATION IS REVIEWED BY A CHANGE-REVIEW BOARD AND IS APPROVED FOR USE (SEE CONFIGURATION MANAGEMENT, ON PAGE 19)
- DEVICE CONFIGURATION IS BACKED-UP (SEE DATA AND CONFIGURATION BACKUP, ON PAGE 13)

1.28 SYSTEM DOCUMENTATION

DOCUMENTATION OF SYSTEMS IS FOLLOWED BY TAQNYAT TO ELIMINATE RISK OF KNOWLEDGE LOSS, AND TO ASSURE KNOWLEDGE TRANSFER TO AUTHORIZED EMPLOYEES. SYSTEMS DOCUMENTATION MAY BE REQUIRED BY TAQNYAT PERSONNEL OR CONTRACTORS.

ALL SYSTEMS ARE DOCUMENTED AND STORED IN KSA IN AN APPROVED DOCUMENT LIBRARY UNDER HIGH CONFIDENTIALITY:

- SECURED FOR READ-ONLY ACCESS TO AUTHORIZED PERSONNEL ONLY
- SECURED FOR MODIFICATION ACCESS TO AUTHORIZED PERSONNEL ONLY
- STRUCTURED TO PROVIDE VERSIONING CONTROL

DOCUMENTATION INCLUDED:

- TAQNYAT PROCESSES AND THE EQUIPMENT NEEDED
- SYSTEM CONFIGURATION
- USER ACCESS
- INTEGRATION AND RELATIONSHIP OF COMPONENTS, SYSTEMS, AND DEVICES

1.29 CONFIGURATION MANAGEMENT

INDUSTRIAL EQUIPMENT REQUIRES SIGNIFICANT EFFORT, SKILL, AND TIME TO DEFINE AND TEST AND MUST BE PROTECTED FROM ACCIDENTAL LOSS OR INTENTIONAL DESTRUCTION ETC.:

- A CHANGE-REVIEW BOARD ARE ESTABLISHED AND TAKE RESPONSIBILITY FOR CONFIGURATION SETTINGS MANAGEMENT, REVIEW, APPROVAL, AND DOCUMENTATION OF REQUESTS, RISK ANALYSIS, RECOMMENDATIONS, AND DECISIONS MADE ETC.
 - CHANGES TO CONFIGURATION SETTINGS MUST GO THROUGH A REVIEW PROCESS WITH THE CHANGE-REVIEW BOARD TO ASSURE SAFETY, ACCURACY, AND EFFICIENCY, WHILE REDUCING RISK WITH THE UPPER MANAGEMENT ENGAGEMENT
 - ONLY APPROVED PERSONNEL MAY CHANGE CONFIGURATION SETTINGS AFTER RECEIVING WRITTEN APPROVAL FROM THE MANAGEMENT BOARD
 - ANY CHANGES MADE TO CONFIGURATION SETTINGS ARE DOCUMENTED.
 - CONFIGURATION SETTINGS ARE BACKED-UP (SEE DATA AND CONFIGURATION BACKUP ON PAGE 13)

1.30 MONITORING AND CONTINUOUS IMPROVEMENTS

THE IMPLEMENTATION OF AN I-ISMS WILL NOT ELIMINATE THE POTENTIAL OF CYBER-ATTACKS OR SABOTAGE FROM MALICIOUS EMPLOYEES. THEREFORE, MONITORING OF THE COMPLETE PROGRAM IS REQUIRED IN ORDER TO IMPROVE THE EFFECTIVENESS OF THE CONTROLS PUT IN PLACE.

- SUPERVISION OF OVERALL MONITORING ASSIGNED TO A PRINCIPAL ENGINEER

THE FOLLOWING IS REQUIRED FOR MONITORING PROCESSES AND LOGS TO DETECT BREACHES:

- DAILY REVIEWS OF COMPUTER SYSTEM SECURITY INFORMATION (ALERTS, LOGS, EMAILS, ON-SCREEN REPORTS ETC.) BY MINIMUM, ASSIGNED TO A COMPETENT AND RESPONSIBLE ENGINEER
- FREQUENT REVIEWS OF INDUSTRIAL EQUIPMENT ACCESS AND LOGS (WHERE POSSIBLE) WITH A MINIMUM OF 1 REVIEW PER WEEK.

- SUMMARY REPORTS TO BE PROVIDED IN REGULAR ENGINEERING TEAM MEETINGS

THE MONITORING OF THE I-ISMS PROGRAM IS DESCRIBED IN SECTION REVIEW AND AUDIT, ON PAGE 5.

1.31 SECURITY BREACH & INCIDENT MANAGEMENT

SECURITY BREACHES VARY BY TYPE, SUCH AS THE UNAUTHORIZED ACCESS TO DATA/SYSTEMS, THEFT OR MODIFICATION OF INFORMATION, SABOTAGE FROM AN EMPLOYEE, OR VIRUS/MALWARE ATTACK.

THE DETECTION OF A SECURITY BREACH REQUIRES:

- INFORM THE ICT CYBER CRIME AND SUBMIT THE NEEDED FORMS
- IMMEDIATE ATTENTION AND ESCALATION TO THE PRINCIPAL ENGINEER IN CHARGE
- IMMEDIATE ATTENTION AND ESCALATION TO THE MOST SENIOR PERSON AVAILABLE
- FOLLOW THE PLAN IN THE RISK REGISTER, AS APPROPRIATE