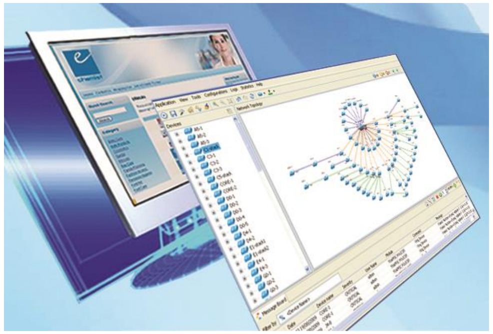
YOUR QUALITY PARTNER FOR SOFTWARE SOLUTIONS

TMA SOLUTIONS

Security & Intellectual Property Protection



Overview

- Certified ISO 27001:2013
- Meet security requirements from global clients
- Passed all security audits from large clients
- Dedicated security group and regular audits
- Certificates: CEH, CISA, CISM

Summary

Physical Security

- 24/7 security guards
- 24/7 power supply
- Magnetic ID card authentication
- CCTV

Network Security

- Secured, separate subnet for each client (VLAN level), , no cross-subnet access
- VPN available between TMA and client
- Firewall with integrated IPS (Intrusion Protection System)
- Anti-virus software for all computers
- Virus screening of all incoming & outgoing emails
- All software are scanned for virus before delivery

Human Resources & Organization

- Mandatory security training for all new hires
- NDA agreement signed by all staff
- Dedicated security group (certified CEH, CISA, CISM) and regular audits

Data Security

- No storage media (USB, CD, DVD) allowed
- File transfer outside the company not permitted
- Firewall system and log checking

Backup/Recovery

- Business Continuity Plan (BCP) for the whole company and Operational Continuity Plans (OCP) for each project
- Data backup plan for each project
- Redundant network backbone and Internet links
- Network based backup system, cross-site storage

Multi tenancy policy and setup

- Physical security
  - Separated and secured working room with magnetic card authentication
  - Only authorized employees are allowed to access the room
  - Access rights are reviewed quarterly
- Network security
  - Separated and secured IP subnet at VLAN level
  - Network gateway (EdgeRouter) with built-in firewall, no cross subnet access is allowed
  - Site-to-site IPSec VPN for direct access to/from customer site

Data sovereignty and protection

- Information assets are classified, labeled and handled according to Asset Management Policy
  - Responsibility for assets
  - Information classification
  - Information labeling and handling
- Only authorized staffs are allowed to access data of customers according to Access Control Policy
- All employees have to sign NDA on first day
- All data is stored on on-premises server
- Currently, we are not handling for kinds of private data of customers

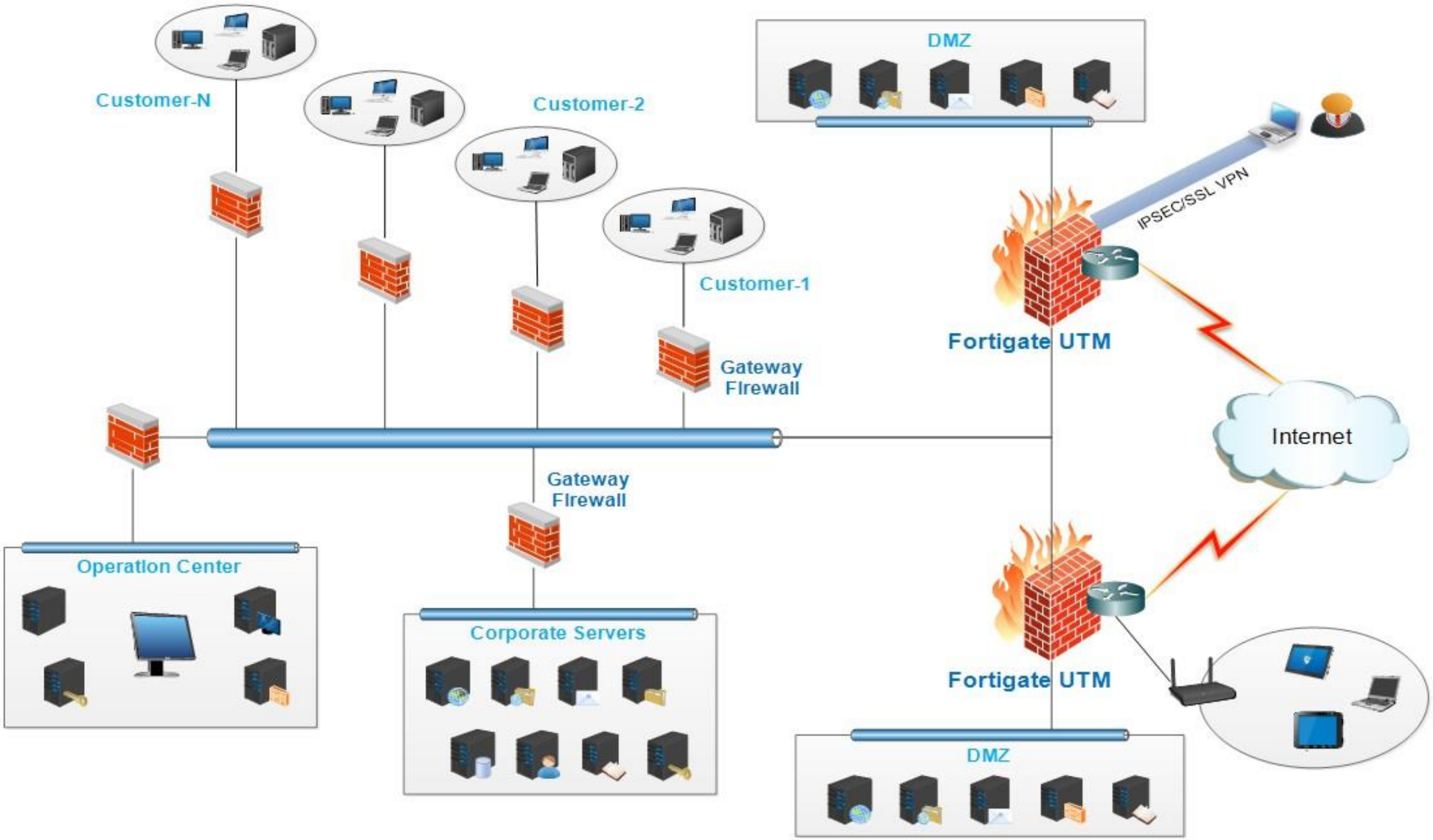
Network infrastructure security

- Firewall infrastructure: external (internet facing) with DMZ using Fortigate, internal firewall in front of every subnet using Linux iptables
- Fortigate network based IDS/IPS for external firewall, DMZ. Snort network IDS for corporate servers. OSSEC host based IDS for DMZ servers
- Antivirus: MacAfee AV on all Windows PCs/servers, centralized managed, automatically update daily, scheduled scan weekly
- Centralized logging system with syslog-ng
- Network monitoring and alerting with Nagios
- Monthly vulnerability scan with Nessus, OpenVAS
- Data-Loss-Prevention at external firewall level (Fortigate) and desktop level (McAfee HostDLP)

Business Continuity Planning

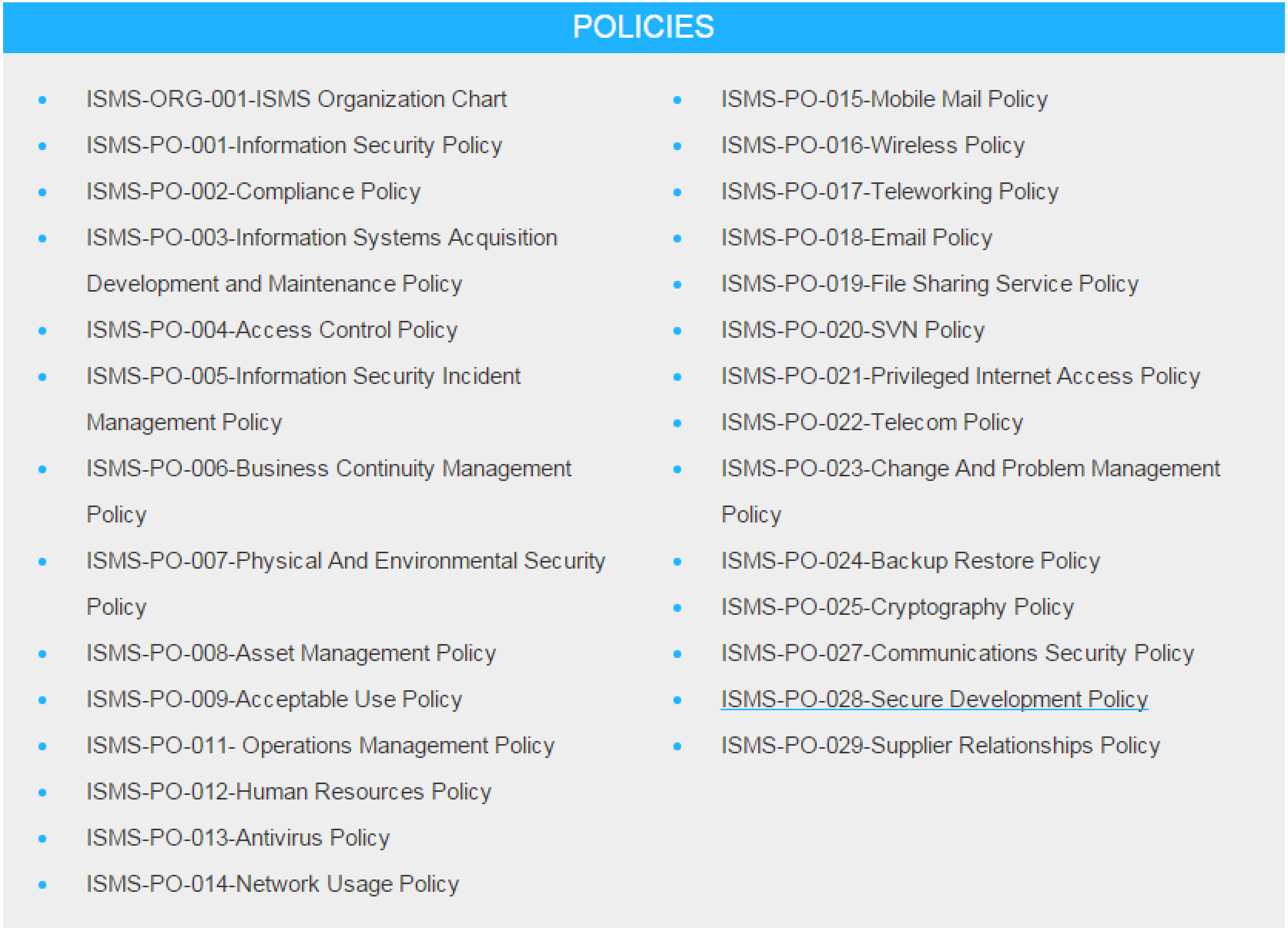
- Corporate Business Continuity plan includes detail of:
  - Response plan
  - Critical business missions
  - Risk Assessment
  - Preventive/Mitigation plan
  - Resumption plan
  - Restoration plan
  - Operation Continuity Plan (OCP) list
  - BCP team members
  - BCP calling tree
- Backup and recovery
  - Automated backup system with cross-site storage
- BCP and DRP are tested annually

Security Topology



- Separate sub-net for each customer
- Multi-layers security

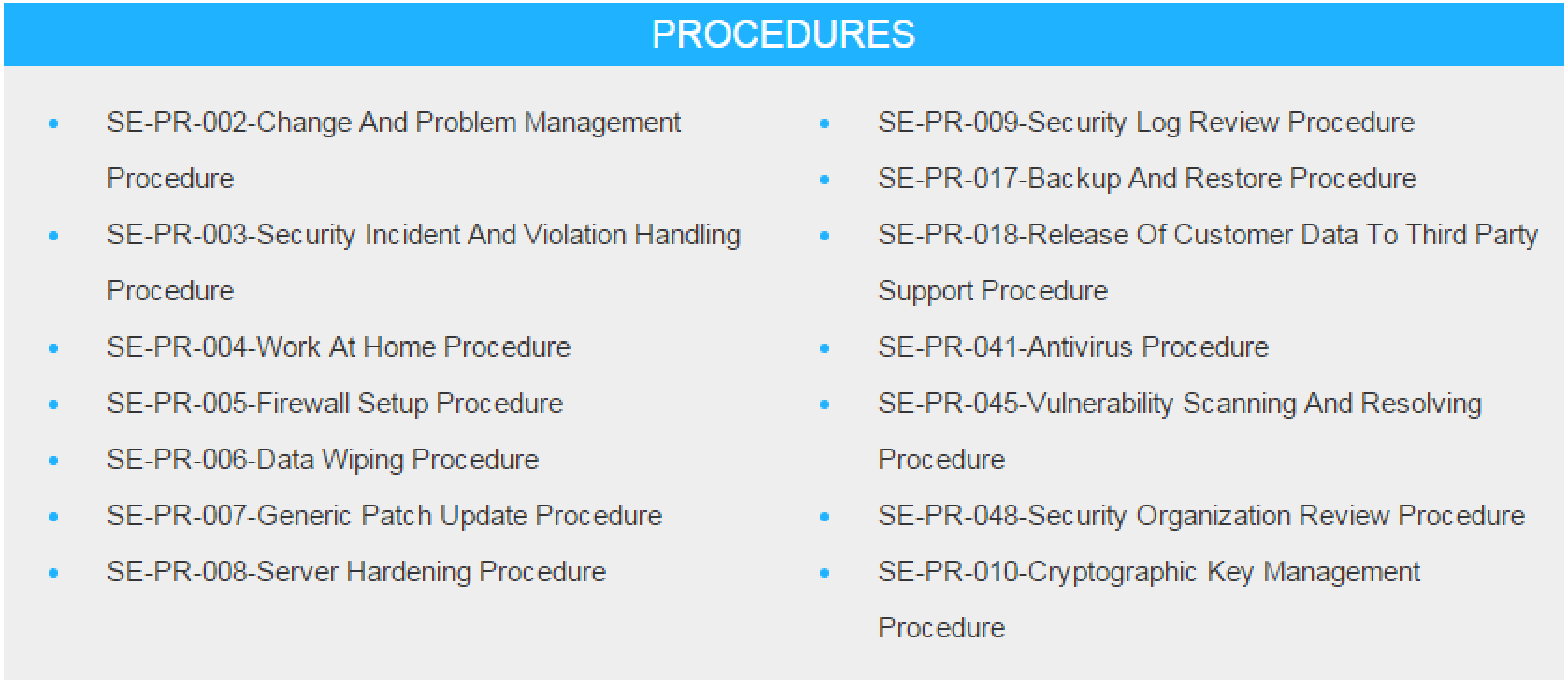
Information Security Management System (ISMS)



POLICIES

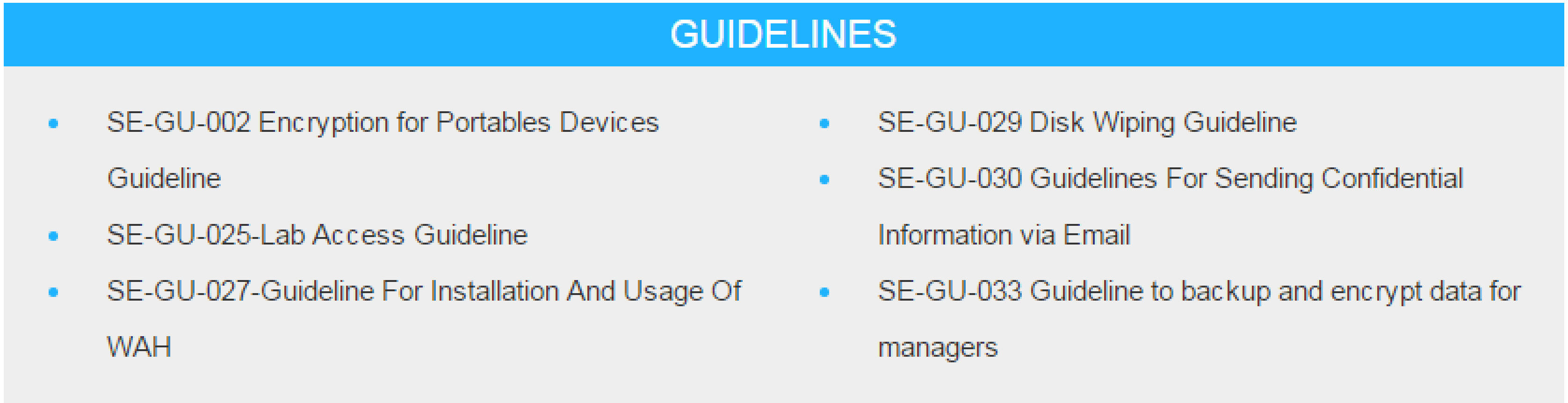
- ISMS-ORG-001-ISMS Organization Chart
- ISMS-PO-001-Information Security Policy
- ISMS-PO-002-Compliance Policy
- ISMS-PO-003-Information Systems Acquisition Development and Maintenance Policy
- ISMS-PO-004-Access Control Policy
- ISMS-PO-005-Information Security Incident Management Policy
- ISMS-PO-006-Business Continuity Management Policy
- ISMS-PO-007-Physical And Environmental Security Policy
- ISMS-PO-008-Asset Management Policy
- ISMS-PO-009-Acceptable Use Policy
- ISMS-PO-011- Operations Management Policy
- ISMS-PO-012-Human Resources Policy
- ISMS-PO-013-Antivirus Policy
- ISMS-PO-014-Network Usage Policy
- ISMS-PO-015-Mobile Mail Policy
- ISMS-PO-016-Wireless Policy
- ISMS-PO-017-Teleworking Policy
- ISMS-PO-018-Email Policy
- ISMS-PO-019-File Sharing Service Policy
- ISMS-PO-020-SVN Policy
- ISMS-PO-021-Privileged Internet Access Policy
- ISMS-PO-022-Telecom Policy
- ISMS-PO-023-Change And Problem Management Policy
- ISMS-PO-024-Backup Restore Policy
- ISMS-PO-025-Cryptography Policy
- ISMS-PO-027-Communications Security Policy
- ISMS-PO-028-Secure Development Policy
- ISMS-PO-029-Supplier Relationships Policy

Security Procedures & Guidelines



PROCEDURES

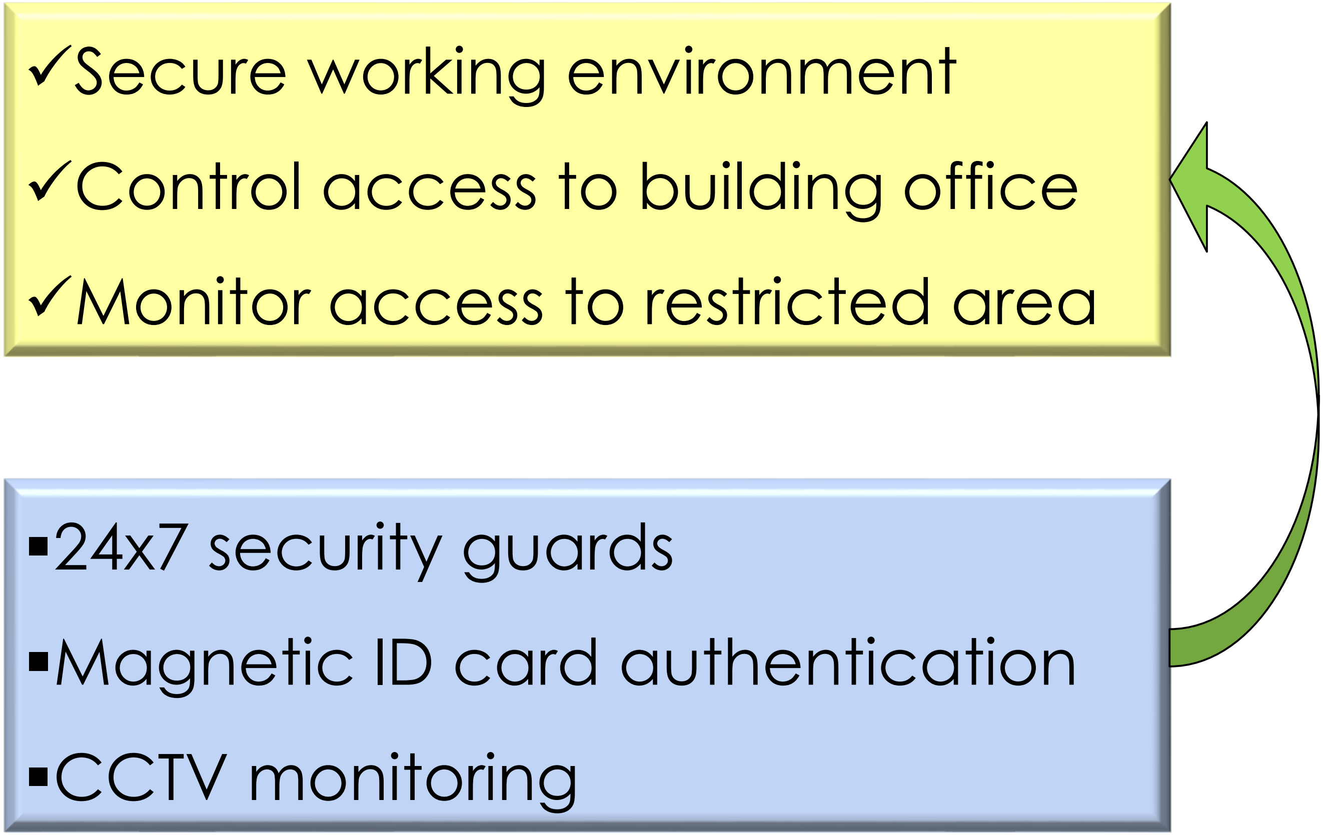
- SE-PR-002-Change And Problem Management Procedure
- SE-PR-003-Security Incident And Violation Handling Procedure
- SE-PR-004-Work At Home Procedure
- SE-PR-005-Firewall Setup Procedure
- SE-PR-006-Data Wiping Procedure
- SE-PR-007-Generic Patch Update Procedure
- SE-PR-008-Server Hardening Procedure
- SE-PR-009-Security Log Review Procedure
- SE-PR-017-Backup And Restore Procedure
- SE-PR-018-Release Of Customer Data To Third Party Support Procedure
- SE-PR-041-Antivirus Procedure
- SE-PR-045-Vulnerability Scanning And Resolving Procedure
- SE-PR-048-Security Organization Review Procedure
- SE-PR-010-Cryptographic Key Management Procedure



GUIDELINES

- SE-GU-002 Encryption for Portables Devices Guideline
- SE-GU-025-Lab Access Guideline
- SE-GU-027-Guideline For Installation And Usage Of WAH
- SE-GU-029 Disk Wiping Guideline
- SE-GU-030 Guidelines For Sending Confidential Information via Email
- SE-GU-033 Guideline to backup and encrypt data for managers

Physical Security



❖ **GOALS**

✓Secure working environment

✓Control access to building office

✓Monitor access to restricted area

❖ **PRACTICES**

▪24x7 security guards

▪Magnetic ID card authentication

▪CCTV monitoring

Human Resources & Organization

❖ **GOALS**

✓Ensure all employees are educated and fully aware about security requirements

✓Ensure information security is managed effectively

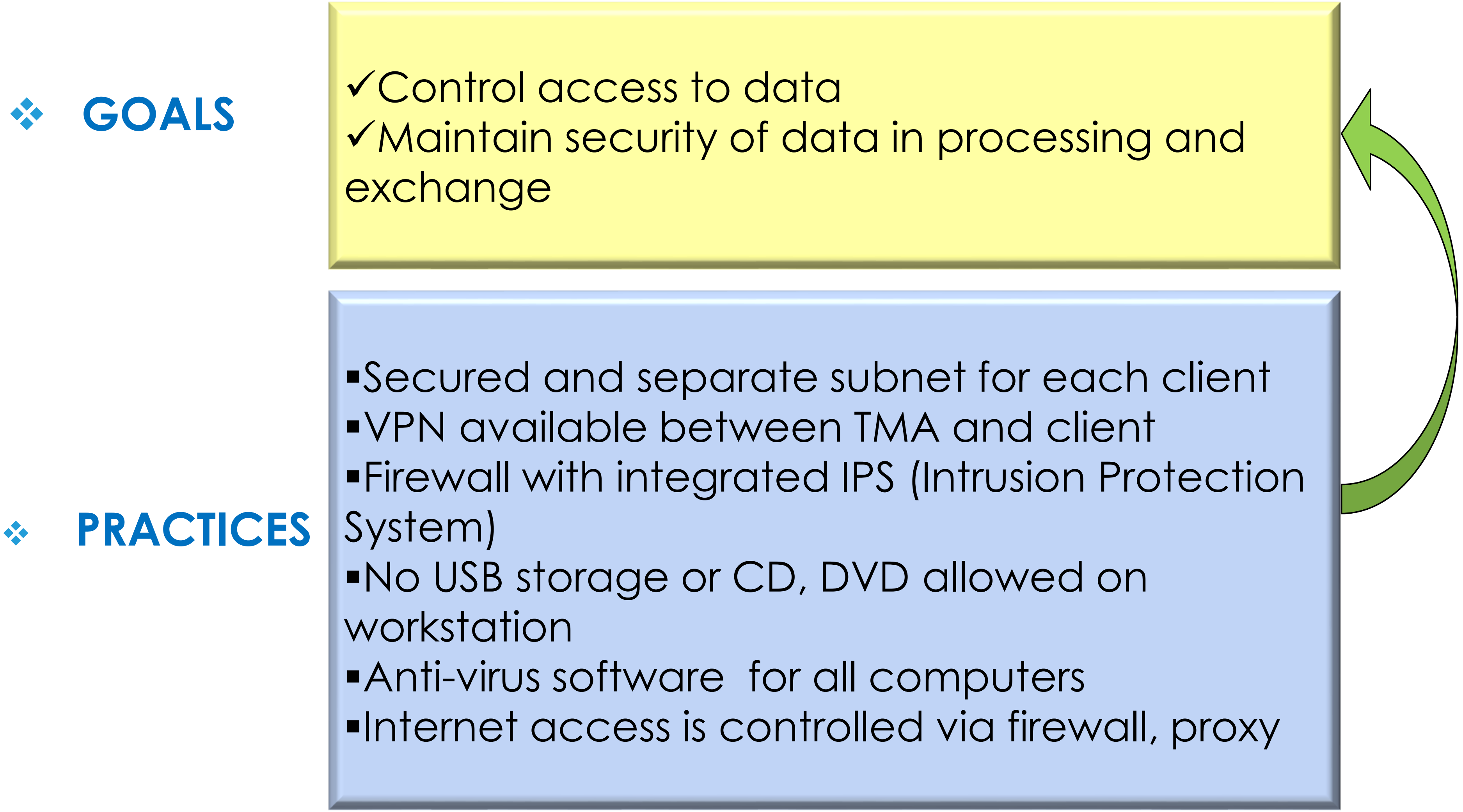
❖ **PRACTICES**

▪Mandatory security awareness training for all new hires

▪NDA agreement signed by all staff

▪Dedicated security group (certified CEH, CISA, CISM) and regular audits

Data Security



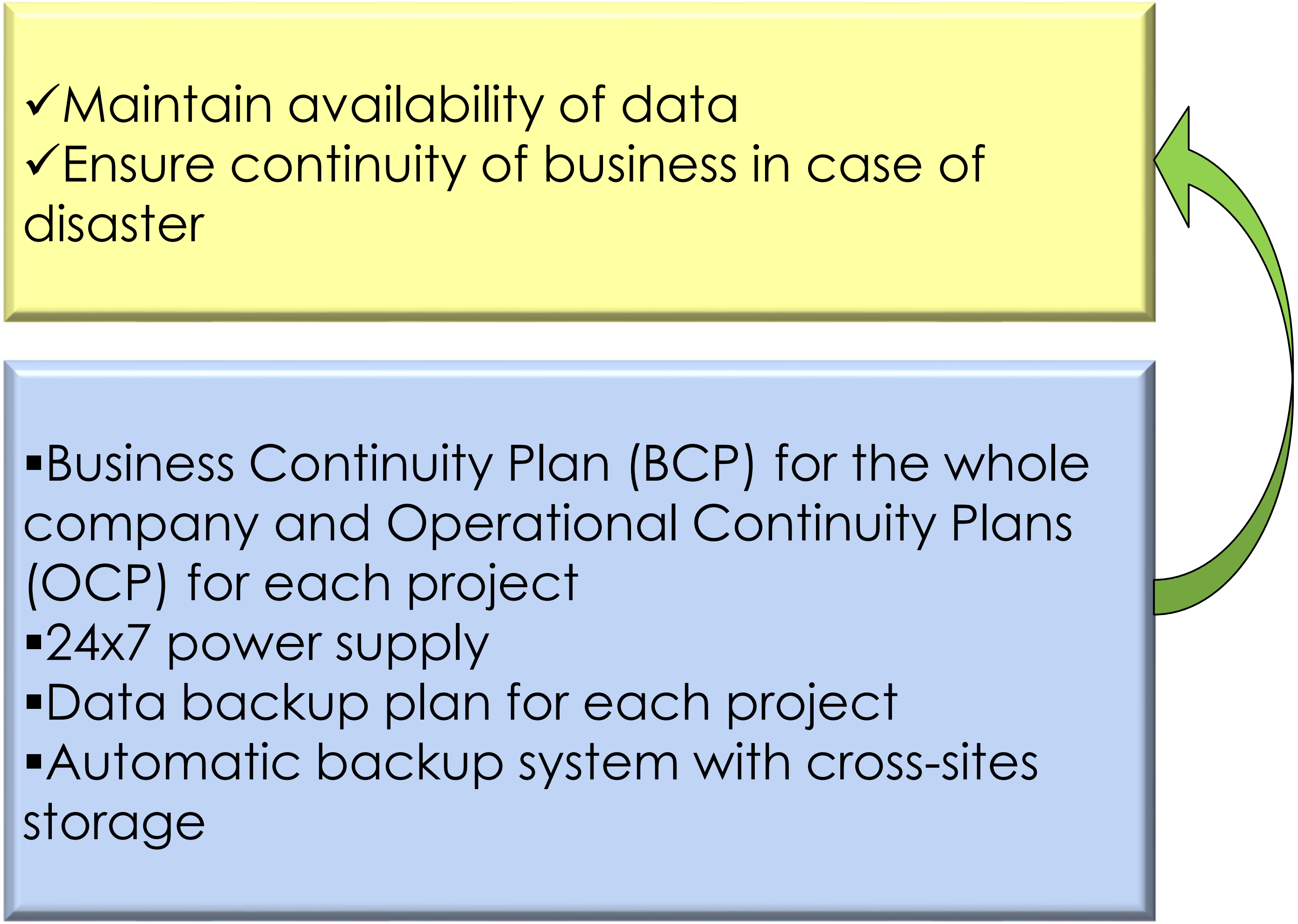
❖ GOALS

✓Control access to data
✓Maintain security of data in processing and exchange

❖ PRACTICES

▪Secured and separate subnet for each client
▪VPN available between TMA and client
▪Firewall with integrated IPS (Intrusion Protection System)
▪No USB storage or CD, DVD allowed on workstation
▪Anti-virus software for all computers
▪Internet access is controlled via firewall, proxy

Backup/Recovery



❖ **GOALS**

✓Maintain availability of data
✓Ensure continuity of business in case of disaster

❖ **PRACTICES**

▪Business Continuity Plan (BCP) for the whole company and Operational Continuity Plans (OCP) for each project
▪24x7 power supply
▪Data backup plan for each project
▪Automatic backup system with cross-sites storage