TeleMessage

10 Top Enterprise Security Best Practices

At TeleMessage, we handle sensitive client information as part of our business, and we've been forced to evaluate and implement specific security technologies, measures, policies and protocols to protect our customers' data.

We've compiled this list of best policies and protocols practices concerning enterprise security based on our security policies.

These helped us pass security and corporate audits, so we believe they represent 10 of the highest priority and most frequently recommended security practices as a place to start for today's operational systems.

These practices address dimensions of information security such as policy, process, people, and technology, all of which are necessary for deployment of a successful security process.

We recommend that you evaluate the security processes at your organization and develop your own policies and procedures (this is especially helpful during an audit).

Furthermore, in addition to making staff acknowledge any documents by reading and signing them, it is key to ensure that they have read and actually understood the policies in question. The best way of achieving this is to provide relevant and engaging training to reinforce the messages and bring the policy alive with current local examples.

1. GENERAL MANAGEMENT:

Managers throughout the organization should consider:

- Information security a normal part of their responsibility and the responsibility of every employee.
- Clearly defining and assigning information security roles and responsibilities and ensure adequate resources are allocated.
- Actions which include visible sponsorship and direction, written communications, and staff meeting time on this subject.
- Creating, enforcing, and regularly reviewing security policies.

2. POLICY:

- Develop, deploy, and enforce security policies that satisfy business objectives.
- Create policies that address key security topic issues such as:
  - Security risk management,
  - Critical asset identification,
  - Physical security
  - System and network management

  - Authentication and authorization
  - Access control
  - Vulnerability management,
  - Incident management
  - Awareness and training
  - Privacy.
  - Ensure that the intent of each policy is reflected in the standards, procedures, practices, training, and security architectures that implement it.

3. RISK MANAGEMENT:

- Periodically conduct an information security risk evaluation that identifies:
  - Critical information assets
  - Threats to critical assets
  - Asset vulnerabilities and risks
- Develop and implement a risk mitigation plan resulting from the evaluation
- Ensure that there is regular review and management of the risks

4. SECURITY ARCHITECTURE & DESIGN:

- Generate, implement, and maintain enterprise-wide security architecture, based on satisfying business objectives and protecting the most critical information assets.
- Deploy a layered approach, including the practices that follow.
- Use diversity and redundancy solutions for high-risk/high-reliance systems.

5. USER ISSUES

ACCOUNTABILITY AND TRAINING:

Users include all those who have active accounts, including employees, partners, suppliers, and vendors. Users consider information security to be a part of their responsibilities, receive training in all policy topics, and consequences related to policy violations.

- Establish accountability for each user action
- Train for accountability and enforce it as reflected in organizational policies and procedures.

ADEQUATE EXPERTISE:

Ensure that there is adequate in-house expertise or explicitly outsourced expertise for all supported technologies (e.g. host and network operating systems, routers, firewalls, monitoring tools, and applications software), including the secure operation of those technologies.

6. SYSTEM AND NETWORK MANAGEMENT:

Ensure proper access controls are in place in systems (i.e., user IDs and passwords that are unique and forced to be changed frequently by the system).

ACCESS CONTROL:

Establish a range of security controls to protect assets residing on systems and networks by using the following tools:

- Access controls, data encryption and virtual private network technologies as required.
- Perimeter and internal security applications that implement security policy.
- Removable storage media for critical data.
- Deploying a system discard process that eradicates all data from disks and memory prior to disposal.

SOFTWARE INTEGRITY:

Regularly check for

- The integrity of installed software.
- And eradicate all viruses, worms, Trojan horses, other malicious software, and unauthorized software.
- And compare all file and directory cryptographic checksums with a securely stored, maintained, and trusted baseline.

SECURE ACCESS CONFIGURATION:

- Provide procedures and mechanisms to ensure the secure configuration of all deployed assets throughout their life cycle of installation, operation, maintenance, and retirement.
- Apply patches to correct security and functionality problems.
- Establish and maintain a standard, minimum essential configuration for each type of computer and service.
- Create a network topology diagram and ensure it is kept up to date.
- Enable adequate levels of logging.
- Perform vulnerability assessment and address vulnerabilities when identified.

BACKUPS:

- Mandate a regular schedule of backups for both software and data.
- Validate software and data before and after backup.
- Verify the ability to restore from backups.

7. AUTHENTICATION & AUTHORIZATION:

USERS:

- Implement and maintain appropriate mechanisms for user authentication and authorization when using network access from inside and outside the organization.
- Ensure these are consistent with policies, procedures, roles, and levels of restricted access required for specific assets.

REMOTE AND THIRD PARTIES:

- Protect critical assets when providing network access to users working remotely and to third parties such as contractors and service providers.
- Use network-, System-, file-, and application-level access controls and restrict access to authorized times and tasks as required.

8. MONITOR & AUDIT:

- Use appropriate monitoring, auditing, and inspection facilities and assign responsibility for reporting, evaluating, and responding to system and network events and conditions.
- Regularly use system and networking monitoring tools and filtering and analysis tools, and examine the results.
- Respond to events that warrant action
- Ensure that all employees know who to contact when they notice suspicious behavior.

9. PHYSICAL SECURITY:

- Control physical access to information assets and IT services and resources.
- Use physical access controls where required.
- Use password-controlled electronic locks for workstations, servers, and laptops that are enabled upon login and after specified periods of activity.
- Control access to all critical hardware assets.

10. CONTINUITY PLANNING & DISASTER RECOVERY:

Develop business continuity and disaster recovery plans for critical assets and ensure that they are periodically tested and found effective.

Elements of a BC plan, at a minimum, should include, but are not limited to, the following:

a. Procedures for response and recovery that contain predetermined prioritized actions on how to:

- Respond to a disruptive event
- Activate the plan
- Recover critical business processes
- Restore the business back to its state before the incident or disaster occurred

b. Alternate work locations and work procedures (if necessary) must be identified in case the primary site is unavailable. The plan should also include procedures to equip the alternate work site (telecommunication systems, PCs, and other devices), and contracts with third parties.

- Procedures to safeguard and reconstruct the home site.
- Procedures to safeguard the alternate site.
- Reconstruction plans for the recovery of all systems resources at the original location.
- Critical information (such as current names, telephone/pager number of key personnel, etc) on continuity teams, affected staff, customers and suppliers.
- Major upstream / downstream applications that contain information system groups that may be affected and critical contact information must be identified.
- Time frames for restoring systems to ensure required transaction processing times are met and disruption time is minimized.

Elements of a DR plan, at a minimum, should include, but are not limited to, the following:

- The identification of possible disasters that could interrupt access to systems for long periods of time.
- Directions to Off-Site Storage locations
- Business recovery location
- Disaster recovery organization chart/list – action team call tree for internal contacts and their locations
- Hardware and other required inventory needed in the event of a disaster
- Application and other required inventory needed in the event of a disaster
- Operating system and other required inventory needed in the event of a disaster
- Vendor name(s) and contact information
- Media, records, and documentation needed for restoration
- Recovery procedures and priority of servers, applications, and other dependent systems
- Time frames for restoring systems to ensure required transaction processing
- Critical file and work in process assessment report
- Recovery status report

TeleMessage

TeleMessage Company Profile

TeleMessage provides business mobile messaging products. Our solution keeps information secure, ensures reliability, allows for management and administration of messages and increased productivity and efficiency.

The TeleMessage enterprise mobile messaging platform is:

Secure – with TeleMessage, messages and chat conversations are encrypted and password protected. We offer end-to-end encryption, password protection, time-limited messages, forward-locking, remote auto lock and wipe in case of theft or lost mobile devices, and advanced delivery confirmations.

Managed – TeleMessage allows you to administer, control, and enforce messaging & information transfer policies. The system includes an administrator interface, message archive, report generator and integrated company address book.

Reliable – TeleMessage makes sure that messages are received by the intended recipient worry-free. All IP Push Notifications that are not received within in a timely manner can be sent as a standard SMS message. We've also invested in our carrier-grade infrastructure, cross-carrier and cross-device message transmission, and emergency notification alert systems. We guarantee 99.95% SLA uptime.

IT-Ready – we've developed a range of APIs that can connect TeleMessage to any IT system in order to send messages, including REST, SOAP, XML, HTTP, and more. You can find all of our API documentation and developer resources on our Developer's Zone.

The solution includes a web portal, Android/iOS mobile apps, and Outlook Plug-In to send IP Push Notifications, SMS, voice, fax and email messages.

TeleMessage has been providing state-of-the-art messaging solutions since 1999. Our software has been successfully deployed and used by thousands of enterprises, trusted by dozens of telecom operators, reaches hundreds of millions of users and powers billions of messages through customers' networks. We support an ever growing number of enterprises, including leading brands across a range of industries such as healthcare, travel, finance and retail, among others.

TeleMessage is a fully owned subsidiary of Messaging International Plc, a publicly traded company on the London Stock Exchange under the symbol "MES".

Contact Us

To learn more about our business messaging platform, please contact us: sales@TeleMessage.com