John Oakey and Mohan Limited

Information Security Policy

We commit to put in place and proactively manage an Information Security Management System (ISMS) designed to protect the Confidentiality, Integrity and Availability of business information, information processing facilities and to provide a secure work environment to our employees and interested parties.

We believe in continually improving our management system by periodically reviewing our ISMS and its associated controls.

We have established a Team to provide management support for information security objectives within the company and strive to develop and implement relevant and cost-effective information security controls by:

- Classifying all business, client and cyber information as per sensitivity;
- Proactively assessing information assets risks and implementing;
- practical and cost-effective controls to mitigate identified risks;
- Controlling changes to information systems;
- Handling security, incidents through an efficient incident response process;
- Complying with applicable legal, regulatory, contractual and other requirements;
- Identifying, building and maintaining the competency of our employees to effectively manage the policy requirements;
- Providing continuous information security awareness and education to employees and stakeholders;
- Preventing interruption to business processes by implementing Business continuity program;
- Continuously monitoring all information system to detect and prevent unauthorized activities;
- Periodically reviewing this policy for its continued suitability and applicability;
- Providing adequate resources required to manage and support effective implementation of this policy.

Incident Management Policy

This policy provides the formally documented expectations and intentions used to direct decision making and ensure consistent and appropriate development and implementation of processes, standards, roles, activities, etc., with regard to this policy.

PURPOSE

The purpose of this policy is to ensure that any incidents that affect the daily operations of the IT Environments of company are managed through an established process. This policy will utilize the best practice framework for the implementation of Incident Management within the company.

Incident Management is the process that defines an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also considered an incident.

The goal of Incident Management is to restore the IT service to its normal operation within agreed service level targets and to manage unplanned events which result in the following:

- Interruption to the normal operation of an IT service.

- Report or notice of a reduction in the quality of an IT service.
- Failure of a Configuration Item that has not yet impacted an IT service.

SCOPE

This policy applies to all company personnel involved in activities that cause or require changes to technology solutions within the company environments. Therefore, the scope of the Incident Management Policy includes the following:

- All IT Supported locations
- All environments subject to the Incident Management Policy determined Company
- Company owned Incidents (e.g., Incidents recorded and managed to closure by IT personnel)
- All items not specifically listed within the Scope section are deemed "Out-of-Scope."

POLICY

The policy is established for Incident Management:

1. IT department must use the currently approved documented incident management process and will be reported, recorded, managed, and appropriately communicated through the approved Incident Management tool.
2. All IT /Application Managers are responsible for ensuring the Incident Management Process is followed.
3. Upon resolution of an incident, the end user will be notified that the incident has been resolved and restored to normal business function.

EXCEPTIONS

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by-case basis. Exceptions shall be permitted only after documented approval from the IT team.

POLICY COMPLIANCE AND MONITORING

Incidents will be reviewed on a periodic basis by the Incident Management Process Owner to audit policy compliance. This is to ensure that the procedures, guidelines, and standards set forth in the Incident Management Process are adhered to.

POLICY REVIEW

The Incident Management Policy will be reviewed on the following basis:

- Annually, by the Incident Management Process Owner
- Upon an update to the Incident Management Process and/or tool
- Upon request of the IT team.

DEFINITIONS

- Configuration Item (Cfg-Item): A service asset component that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and service level agreements.

- Critical Incident (CI): A CI is an abbreviation for the term “Critical Incident” which refers to the highest priority assigned to an Incident. A critical incident is defined as an incident whose impact is extensive or widespread, affects multiple locations, has a potential for a significant loss of revenue or a significant impact to other business operations, with no workaround available. The target for restoration for this priority is As Quickly As Possible (AQAP) or no longer than 2 hours.
- Incident: An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also considered an incident.
- Incident Management: The process responsible for managing the lifecycle of all incidents. The objective is to restore normal operations within agreed service level targets with the least possible impact on either the business or the user.
- Incident Manager: The person or group that is assigned the responsibility of managing the lifecycle of an incident, as defined within the Incident
- Management process.
- IT Service: An IT service is made up of a combination of information technology, people, and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement.
- IT Team: An executive body responsible for the guidance and direction of IT Service Management.

IT Change Management Policy

Definition

IT Change Management is the process of requesting, developing, approving and implementing a planned or unplanned change within the IT infrastructure. It begins with the creation of a Change Request within the Company Application. It ends with the satisfactory implementation of the change and communication of the result of the change to all interested parties.

Process

Formally request a change – All requests for change within the Company Application will be documented by creating a new change request. The change request will be completed by the change requestor with assistance from a member of the ERP staff.

Analyze and Justify Change – The change requestor and the ERP Staff will work to develop a specific justification for the change and identify the impact on infrastructure, business operations and budget, identify business as well as technical risks, develop technical requirements, and review specific implementation steps. The change requestor with assistance from the ERP Staff will be required to submit a functional test plan that is sufficiently detailed to provide assurance that the change will have the desired result.

Approve and Schedule the Change – The ERP Project Manger will chair a Change Management team consisting of – at a minimum – representative IS members from Network Engineering, Server Administration, Operations, Applications Support, Security Administration, Database Administration, Desktop Support, and with appropriate members of the affected end-user community. The group will assess the urgency and impact of the change on the infrastructure, end user productivity and budget. In the event of a major or significant change the change request must be approved by the Director and, where appropriate as determined by the Director or on recommendation by the Change Management team, members of end-user management.

Plan and Complete the Change – The Change Management Team will assign specific IS members and identify appropriate end-user members to complete the change in a manner that will minimize impact on the infrastructure and end users. In the event that the change does not perform as expected or causes issues to one or more areas of the production environment, the team will determine if the change should be removed and the production environment returned to its prior stable state.

Post Implementation Review – A review will be conducted by the Change Management team to formally ensure the change has achieved the desired goals. Post implementation actions may include acceptance, modification, or backing-out of the change. The team formally documents the final disposition of the change as part of the Change Request Documentation.

Scope

The intended scope of the change management process is to cover changes to the Company Applications in the production environments.

Primary functional components include the following:

- Hardware – Installation, modification, removal or relocation of computing equipment.
- Database – Changes to databases or files such as updates, additions, reorganizations and major maintenance.
- Application – Application changes being promoted to production as well as the integration of new applications and the removal of obsolete elements.
- Schedule Changes – Requests for creation, deletion or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the ERP Staff.
- Outages – application or network outages in excess of 30 minutes in duration will require a formal review to ensure that issues are identified, notification protocols are followed, and solutions defined.

Out of Scope

Tasks that require an operational process but are outside the initial scope of the ERP Change Management process include:

- Disaster Recovery
- Changes to non-production elements or resources
- Changes within the daily administrative process such as password resets, user adds and deletes, etc.
- Functional configuration of Business Units

Password Policy

Company has created the rules and password security strategies at Admin & User level as per industry standards:

1. Password history should be enabled for at least 7 historic passwords
2. Password validity should be of maximum 60 days
3. Password length should be set at minimum 8 character
4. Password complexity should be enabled
5. Password encryption should be enabled

Password creation

- All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember "can become "TmB0WTr!".
- Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.
- All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up must be changed as quickly as possible.
- Protecting passwords
- Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.
- Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks.
- Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.
- Employees may not use password managers or other tools to help store and remember passwords without IT's permission.

<u>IT Backup Policy</u>

1) IT department of units of the company will take daily backup of their centralise database.
2) Daily backup will be maintained in 3 places.
3) First, in separate drive other than root drive (C:)
4) Second, in separate system in same building.
5) Third, in external device to be stored in remote building.
6) All units will send their weekly and monthly backup to Mohan Nagar.
7) All users will take backup of their working files (excel, word etc.) in separate derive and external device.