Change Capacity and Access Management Policy

Introduction

The purpose of this Change Management Policy is to establish guidelines and procedures for the initiation, review, approval, implementation, and documentation of changes within the company. The policy aims to ensure that changes are managed in a controlled manner to minimize risks, disruptions, and negative impacts on the Company.

Policy statement

The policy will help us to communicate the management's intent. This is to show that changes to Information and Communication Technology (ICT) supported business processes will be managed and implemented in a way that minimises risk and impact to us and our operations. All changes to IT systems shall be required to follow an established change management process. This requires that changes to IT systems be subject to a formal change management process that ensures or provides for a managed and orderly method. This includes the way changes are requested, approved and communicated prior to implementation (if possible), and logged and tested.

Scope

This policy applies to all changes that may impact the organization's information systems, processes, technology infrastructure, or other aspects that contribute to its operational environment. All proposed changes must be documented using the Project and Change Management Proposal Business Case for InfoSec QC396 HR form and follow the SOP23 Project Management for Information Security.

Employees

This policy applies to all parties operating within the Interr's network environment or utilising information resources. No employee is exempt from this policy.

IT Assets

This policy covers the data networks, local servers and personal computers (stand-alone or network-enabled) located at offices and on sites or worked remotely, where these systems are under the ownership of the organisation. This includes any personal computers, laptops, mobile devices and servers authorised to access the organisation's data networks.

Documentation

The policy documentation will consist of CMP and related procedures and guidelines.

Records

Records being generated as part of the CMP shall be retained for a period of 2 years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Change Risks

When assessing a change, a risk assessment is undertaken using the following criteria:

High:

- Previous change has been made and was not successful
- Complex implementation or back-out plans
- Novel technology, not previously implemented

Medium:

- Previous similar changes have occasionally been problematic
- Some complexity to implementation or back-out plans
- Standard technology utilized in a non-standard application

Low:

- Previous similar changes have always been successful
- Simple implementation or back-out plans
- Standard technology used in a BAU context

Change, Capacity and Access Management

Interr Ltd defines a change as anything that alters, modifies or transforms the operating environment of any systems, software or services that has the potential to affect the stability and reliability of in infrastructure or disrupt the business of Interr Ltd or its clients.

Any change may have the potential to impact information security, and therefore consideration as to whether this is the case must be made prior to implementing the change. The change control process shall include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. This is in line with the SOP 23 Project Management.

Changes may be required for many reasons, including, but not limited to:

- User requests or Client's recommendations
- Changes in regulations
- Hardware and/or software upgrades or hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, change of office layouts, etc)
- Unforeseen events or periodic maintenance

Each Information Technology request, including emergency requests for Change will be reviewed and prioritized by the ISO/CEO following discussion with senior management.

These changes will be monitored by the Super Admin User after receiving an approval from the CEO. All changes will undergo some level of testing depending on the complexity of the change.

During the testing process, Interr will determine that the change satisfy specified requirements, and demonstrate that it is fit for purpose and use. All testing will be completed using set up of fictitious users prior to the actual roll out of a new system or a service.

Testing may be performed by the team(s) who develop the software or by a temporary team of testers composed by selected Head Office individuals from different existing teams.

No new services, software or systems being introduced or changed will be implemented until all testing has been completed to a satisfactory level and assigned to the relevant access groups.

Security requirements – analysis and specification

Whilst Interr doesn't design our own systems or creates enhancements to our existing information systems, we use external systems as part of our service delivery and recognise the importance of protecting the security information held within these systems.

All security requirements shall be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall functional requirements for an information system as stated in the SOP23 Project Management and Change Management.

Statements of functional requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls needed to ensure the confidentiality, integrity and data availability for the information system. These specifications should consider the automated controls to be incorporated in the information system, and the need for supporting procedural controls, as listed on Interr's Data Risk Treatment Plan and Register.

All new information processing systems shall be required to be approved by the executive board of directors. Access provisioning, authorisation process and duties and responsibilities of all relevant users will be communicated and in line with this policy as stated above and the Information handling policy. Requirements of protecting the assets and logs will be in line with the in protection of log information as stated above. Where the security functionality in a

proposed product does not satisfy the specified requirement, then the risk introduced and associated controls required to address the risk should be reconsidered prior to purchasing the product. Where additional functionality is supplied which causes a security risk, this shall be disabled or the proposed control structure should be reviewed to determine if advantage can be taken of the enhanced functionality available.

Any allocation of authentication information shall be handled in a secure way inline with the rest of the company's policies regarding information security.

The implementation plan

The implementation plan details all the stages that are required in order to successfully manage the change, and includes a Test Plan. In more complicated changes this may also include a project schedule and timeline:

1. Review the implementation plan.
2. Make the Data Controller aware of any amendments or changes.
3. Make a note of the timeline and any training or testing, plus how this will affect department staff.
4. Make a note of any dependent tasks. For example, if one department is unable to make a change until another has completed theirs.
5. Authorise the implementation plan by email

Pre-change

Once the implementation plan has been approved, it's important that the staff in each department are made aware of what needs to happen, when and by whom. The Relevant Manager:

- notifies affected Staff of the change and assigns actions and makes them aware of the Roll Back Strategy.
- ensures that Staff who have been allocated Test Actions have copies of the Test Plan and are aware that all test documentation is to be retained.
- leases with other Stakeholders and the Data Controller to ensure that all aspects of the change are progressing as planned.

Post-implementation review

Once a change has been implemented it's important that the situation is reviewed to identify any problems that could be prevented in the future, or improvements that could be made. The Stakeholders will carry out a post-implementation review one month after the change has been promoted to live. This is unless problems or issues present themselves. Two months after the change has been implemented the stakeholders will conduct a further review.

The ISO will review the change documentation and follow up quarterly. The minutes and action points of these reviews are held on file with the change documentation. The internal and external auditors will examine the change management documentation on an agreed time period and their comments and recommendations will be acted upon.

Distribution and Maintenance

The policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the DHRC and system administrators.

Privacy

The policy document shall be considered as 'confidential' and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the CEO and Interr.

Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required
- any risks created by the policy exception
- evidence of approval by all appropriate parties

Policy Review and Assessment

This policy may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024