IT SECURITY AND USAGE POLICY

Policy Document Number	01
Policy Details	Acceptable Usage Policy
Scope	This Policy extends to all desktop computers, laptops, data storage devices, print/copy/scan devices, communication and network devices and other information systems owned or leased by the HRPL's. All permanent/contract employees of the HRPL's and Third Party Vendors / Outsourced staff who use the HRPL's IT resources.
First Created	v 0.1 – DEC 15TH, 2014
Last Updated Version	1st December, 2023
Latest Version	1st July, 2024
Created by	Tanaji Chaudhari (Manager - IT)
Approved by	Anand Tomar (General Manager – IT)

#1. INTRODUCTION & POLICY STATEMENT

This policy aims at clarifying users' rights, rules and responsibilities regarding HRPL's Information assets and services and encouraging their effective usage. Users must adhere to safe usage practices that do not hamper business objectives, bring disrepute to HRPL's or attract legal liability.

#2. STANDARDS AND PROCEDURES

DESKTOP SECURITY

(1) Users are responsible for the security of their desktops / laptops and must take adequate measures to restrict physical and logical access to their desktops / laptops.
(2) All desktops / laptops must be configured by IT as per the secure IT configuration standard.
(3) Users must not change any hardware configuration, settings in the operating system or any applications installed on their desktops / laptops. If users require any change in the hardware (For example HDD/SSD/mouse) or software settings. The request for the same must be routed through department head.
(4) Users must not install any software or applications on their desktop / laptop that is not authorized or not essential to the HRPL's business. In case of additional software requirements, prior approvals have to be obtained from department head & HO IT.
(5) To prevent the risk of unauthorized access, the users must adopt the following measures:
    - Ensure logging out of applications before leaving the work terminal unattended for an extended period of time.
    - Desktop/Laptop/Tablet/Mobiles or any other communication asset must not be left unattended.

In addition to the recommended security requirements for desktops, laptop users must ensure the following:

- When connecting to the internal LAN as well as external networks, ensure that the anti-virus agent is installed with the latest signature patterns on the laptop.
- Users must consult with the IT Helpdesk Team in case of issues with the systems.
- Inform the loss of laptop to the IT Helpdesk. IT Helpdesk must communicate to the IT HO Team and ensure necessary steps are taken to control the damage.

#3 PERSONAL EQUIPMENT – HANDLING AND SECURITY

Explicit permission must be obtained from the concerned HOD and Head IT for connecting devices (Laptops, Desktops, PDAs, Mobile phones / devices with wireless capability) to HRPL's network in case of:

- Guest or external vendors who are not employees of HRPL
- HRPL Employees personal devices (Laptops, PDAs, Mobile phones / devices with wireless capability).

#4 CLEAR DESK AND CLEAR SCREEN

- Users must ensure that desks, other work areas, photocopiers and other office equipments are kept cleared of papers and any storage media when unattended.
- Computer screens must be kept clear of sensitive information when unattended.
- All workstations located in public areas must have password-locked screen savers enabled to activate after 15 minutes of inactivity.

#4 ANTI-VIRUS

- Users must not change / disable the configurations of the antivirus settings like daily virus scan, definition of server details and update schedules.
- All files received from external sources must be scanned for viruses before opening. This includes files in removable media like CD's, Internet Downloads, Email attachments or files shared through the network.
- The virus signatures must be periodically updated to prevent against new malicious attacks.
- User must report to the IT Helpdesk of any virus detected in the system which is not cleaned by the anti-virus software.

#5 PERSONAL SECURITY

(1) Users must protect the confidentiality of their accounts by having complex passwords. For passwords to be termed as complex, it must have a, combination of the following:
   - Minimum length of Sixteen (16) characters
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Numerals (0 through 9)
   - Non-alphanumeric characters or symbols (e.g.,!, @,$, #, %)

(2) Users must not use the following as their passwords:
   - words found in a dictionary (English or foreign);
   - names of family, pets, friends, co-workers, fantasy characters, etc.;
   - computer terms and names, commands, sites, companies, hardware, software;
   - words derived from organization name such as 'MCD1234' or any derivation;
   - birthdays and other personal information such as names, addresses and phone numbers;
   - word or number patterns like aaabbb, qwerty, zyxwvuts, 1234, etc.

(3) The remember password option if available in applications must be disabled.

(4) Users must not share their passwords with anyone including colleagues, supervisors, auditors and IT staff. Users must also not ask others (including customers and colleagues) for their passwords. All passwords are to be treated as sensitive, confidential information.

(5) Users must ensure that nobody is watching when they are entering password into the system. Users must also not watch when others are entering passwords in their system.

(6) User must not keep a written copy (in paper or electronic form) of password at their workstations / public places.

(7) Users must change their password regularly. While some applications enforce password change and complexity on users automatically, it may not be feasible to enforce it for all accounts and for all applications. Users must change their passwords under any of the following circumstances:

- At least once in 45 days
- As enforced by system (applications and operating system).
- As soon as possible, after a password has been compromised or after the user suspects that a password has been compromised.

(8) All operating systems and applications must be configured to lock out the accounts after 5 successive unsuccessful attempts. User must report to the IT Helpdesk team if account is locked out before 3 successive unsuccessful attempts.

(9) User should not log into the workstation / server using the administrator password without written permission from IT Head. Any user logging into the system using administrator password without permission is liable for disciplinary action.

#6 INTERNET USAGE

(1) Users must access Internet for business purposes and restrict non-business activities over Internet. Occasional and reasonable personal use of Internet services is permitted, provided it does not interfere with work performance.

(2) Employees must access Internet only through the connectivity provided by the HRPL's and not set up Internet access without authorization from the Information Technology Department. Connection to the internet offers an opportunity for unauthorized users to view or access HRPL's information. Therefore, it is important that all connections be secure, controlled and monitored.

(3) All access to Internet must be authenticated and will be restricted to business related sites. HRPL's will have the right to filter and prohibit access to certain websites at its own discretion.

(4) Users must not use Internet facilities to:

- Download or distribute malicious software or tools or to deliberately propagate any virus.
- View sites not related to the area of work.
- Violate any copyright or license agreement by downloading or distributing protected material.
- Upload files, software or data belonging to HRPL's to any Internet site without authorization of the owner of the file/ software/ data.
- Share any confidential or sensitive information of the HRPL's with any Internet site unless authorized by superior/ controller.
- Post views or opinion on behalf of HRPL unless authorized by top management.
- Post remarks that are defamatory, obscene or not in line with HRPL's policy on the subject.
- Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting HRPL.
- Download any unauthorized software.

(5) In case such misuse of the Internet access is detected, HRPL's can terminate the user Internet account and take other disciplinary action.

(6) Users are responsible for protecting their Internet account and password. Users will be held responsible for any misuse of Internet access originating from their account. Users should bring to the notice of IT Helpdesk if any unauthorized software is found on the laptop or any policy is violated.

(7) Users must ensure that security is enabled on the Internet browser as per guidelines given below –

- Configure browser not to remember web application passwords. (In Control Panel > Network and Internet Connections > Internet Options, Click Tools > Internet Options > Content > Auto Complete. Uncheck all options.
- Set browser security setting to medium. (In Control Panel > Network and Internet Connections > Internet Options, Click Tools > Internet Options > Security > Default Level. Set this to Medium)

(8) Users must not access websites by clicking on links provide in e-mails or in other websites. When accessing a web site where sensitive information is being accessed, it is advisable to access the website by typing the URL address manually rather than clicking on a link.

#7 E-mail usage

(1) The electronic mail facility provided by the HRPL's is for official communication only. Use of the HRPL's official mail account for personal purposes is prohibited.
(2) Users will be provided with a fixed amount of Mailbox Storage space and that will be restricted.
(3) Confidential or sensitive information must not be transmitted over e-mail unless it is encrypted or password protected. Users must mark the mail as confidential in the subject line in respect of the e-mail containing sensitive information. Users must exercise caution in protecting the confidentiality while communicating with external entities.
(4) Users owning the email account are responsible for the content of the email originated, replied or forwarded from their account to other users inside or outside the HRPL's. Users are prohibited from sending or forwarding the following categories of email within or outside the HRPL's:
    - E-mails with any libelous, defamatory, offensive, racist or obscene remarks
    - E-mails containing messages that may damage the reputation of the HRPL's.
    - E-mails that contains viruses or worms
    - Unsolicited emails to a large number of users which can be considered as mail spamming
    - E-mails containing any document, software or other information protected by copyright, privacy or disclosure regulation
    - Mails to external entities containing instructions or contents that require authorization of a superior in the normal course of communication, unless such prior authorization is obtained

In case of such misuse of the e-mail system is detected, the HRPL's can terminate the user account and take disciplinary action.

(5) Users must protect their e-mail account on the server through strong passwords and must not share their password or account with anyone. Similarly, all e-mails stored locally on the user's machine must also be password protected.
(6) Users must exercise caution in providing their e-mail accounts or other information to websites or any other Internet forum like discussion board/mailing list. The official account must not be disclosed in blogs and public forums.
(7) HRPL's reserves the right to monitor e-mail messages and may intercept or disclose or assist in intercepting or disclosing email communications to ensure that e-mail usage is as per the recommended guidelines.

#8 SOCIAL MEDIA

(1) Do not post messages that are unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive, confidential or proprietary information about HRPL and Employees
(2) Do not post content copied from elsewhere, for which you do not own the copyright
(3) Do not post the same message, or very similar messages, more than once (also called "spamming")

(4) Do not publicize your, or anyone else's, personal information, such as contact details.
(5) Only authorized users can set up HRPL's accounts on social media sites. Departments that have a social media page or would like to start one should contact communication department to ensure all institutional social media sites coordinate with other HRPL / HRPL's sites and their content.
(6) Social Media sites are monitored and if any content has been added to sites about HRPL's without due permission then appropriate action would be taken.

#9 DOCUMENT AND MEDIA HANDLING

(1) All documents containing sensitive information must be marked as "confidential" both in electronic and print format. Care must be taken to ensure confidentiality while these documents are transmitted over e-mail, fax or other communication channels or during printing and photocopying of documents.
(2) All media used to store confidential/sensitive information must be named, classified and labeled accordingly.
(3) Confidential documents and media must not be kept unattended in the user's work area, near printers or fax machines and must be stored with appropriate physical security controls.
(4) Users must adopt a clean desk policy for papers, diskettes and other media in order to reduce the risks of unauthorized access, loss of and damage to the information outside business hours. Unused documents/papers must be destroyed using shredder machines. Expired and corrupted storage media must be destroyed before disposal.
(5) Sensitive information may get revealed unintentionally due to unsafe practices; care must be exercised in the following scenarios to protect sensitive information:
    - Reading/sharing confidential documents in public places
    - Discussing confidential information in public places
    - Working on laptops in public places
    - Answering to queries over the phone to unverified persons
    - Providing information to vendors/suppliers
(6) Usage of personal removable storage devices is prohibited unless an explicit approval is obtained from the Information Security Group (IT).
(7) Users must ensure that information is removed completely from storage media / asset before any maintenance / repair / disposal activity.

#10 INCIDENT REPORTING

(1) End users must report security incidents (non-application specific) to IT Helpdesk (on high priority) for necessary action.
(2) Users who are system administrators of applications and network devices must additionally report any incidents that fall under the following categories:
    - Unauthorized use of an account (privileged or otherwise)
    - Unauthorized access to directories, files or media
    - Placement of sniffing hardware or software on the network segment to capture data traveling across it
    - Unauthorized modification to data / file contents
    - Denial of Service or disruption to system activity. Such incidents might be due to a distributed denial of service attack through packet flooding or connectivity issues.
    - Unauthorized password resets
    - Loss / Physical damage to systems

#11 SECURITY VIOLATIONS

Certain categories of activities, which have the potential to harm, or actually harm information assets of the HRPL's are defined as security violations and are strictly prohibited. All security violations will entail disciplinary action. Security violations will include the following but are not limited to:

- Introducing viruses on the network
- Computer Impersonation
- Erasing or modifying data on central systems without authority
- Downloading or transmitting objectionable content (through Email or Internet)
- Running scans or attack tools,
- Bypassing access control mechanisms
- Exploiting any system vulnerability
- Installing or disturbing unlicensed software/Operating system
- Vandalism, Computer fraud or theft
- Installation of any software on the machines without approvals.

#12 CONFIDENTIALITY VIOLATIONS

(1) The employee must not, either during or after his employment, divulge or utilize any confidential information of the HRPL's. This will include processes and information on the HRPL's business affairs gathered during the course of his/her tenure.

(2) Except as may be necessary for the purpose of his duties, the employee must not, without the consent of the HRPL's, retain or make copies of:

- Identity Cards, Letters
- Reports, Drawings, Calculations, Formulas
- Agreements, Forms & Licenses
- Other other documents (electronic or paper) of whatever nature belonging to HRPL.

(3) Nor must he/ she retain samples or specimens in which the HRPL's may be or may have been concerned in and which have come into his/her possession by reason of his/her employment.

(4) Employees must not access, copy, divulge or destroy any type of information not in his scope of work, belonging to other employees of the HRPL's.

(5) Employees with access to privileged information must not divulge that information even to other employees or third parties.

(6) Employees who have been assigned the HRPL's assets, E.g. Laptops, PDA's, and Mobile Phones etc. must comply with the statements of confidentiality mentioned above.

(7) Employees must not use their personal IT assets, E.g. Hand Held PC's, Laptops, PDA's etc. to process or record any business information without explicit approvals.

(8) If on the termination of his employment, the employee is in possession of any originals or copies of the above mentioned material, he must return the same to the HRPL's.

#13 PRINT / COPY / FAX / SCAN DEVICE HANDLING

(1) Copies of sensitive documents including printouts, scanned images, fax etc. must not be taken without authorization. Users must ensure that authorized copies of sensitive documents are collected only by authorized personnel.

(2) Unwanted copies of sensitive documents must be destroyed such that the information cannot be reconstructed.

(3) User must take appropriate precautions for ensuring that:

- Unauthorized persons don't access print/copy/scan facilities
- Printouts are collected immediately on firing the print job.
- Spoilt print copies must be destroyed such that they cannot be reproduced
- Documents are not faxed to unattended/unknown fax numbers/email boxes.
- Only required number of printouts and photocopies are taken.

Laptop Policy:

1.1 Objective

The Laptop Policy is designed to assist the Employees to comply with the business objectives even on field and to access company application and mails anywhere to comply with the work Processes.

1.2 Eligibility

This policy is applicable only to all employees who are on rolls with HRPL, Interns and Management trainee. This will include employees on "Field" and "Office" Category.

Department Head has the right to take decision on whether the employee is to be given a laptop or desktop.

1.3 Approval Process:

- For laptop replacements, IT to raise CAPEX and obtain approval before raising the Purchase Order.
- For new joinees, HOD (IT) has the authority to raise the Purchase Order and obtain approvals subsequently basis requisition from the HR department.

1.4 Laptop Issuance Procedure:

- For new joinees, the Laptop request Form is to be completed and submitted to the IT Department by HR atleast 3 weeks in advance from the date of joining of the new employee.
- The status of available laptops will be checked by IT when the request is received.
- IT will allot laptop from existing stock or will arrange for procurement of the new laptop.

1.5 General Rules:

- It is mandatory that the employee handles the laptop carefully and take maximum precautions to avoid any physical damages to the laptop / spilling liquid on the laptop. Repairs of laptop due to any such damages to the laptop will need to be authorized by the Business Council member of the respective department before IT can initiate the repairs. HRPL reserves the right to recover the costs from the employee. Disciplinary action will be taken for any misconduct.
- In case of misplace / theft / total damage due to mishandling of the laptop, HRPL reserves the right to recover the entire cost from the employee.
- Employees are not permitted to delete the Company data on the Laptop and are expected to maintain absolute Confidentiality about the data in total interest of the Company during tenure with the Company.
- HRPL IT authorized representatives can inspect the Laptop, its usage and the data maintained at any time and the employees are required to readily submit the laptop for such inspections.
- Misuse of the laptop like visiting restricted sites, saving unauthorized data are strictly prohibited… Strict action will be initiated against employee if any such activities are found…
- Employee need to carry Laptop daily to the Office without fail and it should be strictly used for Official purpose in the interest of the organization's objectives and priorities.

- Employee will use only licensed software installed by IT on his / her laptop and will be solely responsible for the safe keeping of the data.
- Users are not authorized to install any software on the laptop. Any such request should be through a service request and authorized by the reporting manager. In case of costs it should be approved by respective Department Head.
- It is mandatory for the employee to deploy and adhere to IT policies communicated and implemented by IT from time to time.

1.6 Laptop discontinuation Procedure:

A) CESSATION FROM SERVICE

- On the last working day of the employee, the laptop must be returned to IT. IT will format the laptop and will ensure that all company data back-up is taken and removed from Laptop.
- Formatting of laptop by IT will be mandatory for every laptop before re-allotment to another user.
- IT shall handover the company data to respective person within organization only on formal approval of HOD. Any request from employee will not be entertained.

1.7 INSURANCE

The laptops are covered under insurance for accidental damages, theft / loss due to burglary. In case of theft / loss due to burglary, it is mandatory for the employee to submit FIR to fixed assets team to initiate the insurance process.

1.8 Laptop buyback

1. Every Quarter IT team will publish the user's list whose laptop has aged 5 years.
2. This list will be circulated only with the employees whose laptop has aged 5years, who in turn can purchase these laptops.
3. In case no user is interested in purchasing the laptop, then the laptop will be opened up for sale to the other employees and the communication will be sent to all the employees by IT.
4. The Buyback policy for such 5 years laptop would be as below:
    a. Interested employee to confirm on email on their interest to buy the laptop.
    b. The cost of the laptop will be Rs 7000 (Rupees Seven thousand Only) which can be paid by the employees via cheque or NEFT to Hardcastle Restaurants Pvt Ltd
    c. The old laptop will be handed over to the user in 15 days
5. The maintenance and repair of software and hardware will be sole responsibility of the employee.
6. The employees are recommended to thoroughly check the laptop before purchase to ensure there are no physical damages during the purchase.
7. In case of any physical damage or repairs post the sale of laptop, the employees will be solely responsible for the same.
8. Operating System license is available with each laptop.
9. Other license software including all Microsoft licenses will be removed by IT. In case of any issue with the hardware or software, employee needs to get the same repaired from outside vendors. IT will not be liable for such repairs.

10. Asset inventory will be updated and managed by IT.

1.9 Policy Violations

Violations of the policy could result in disciplinary action, including termination of employment. Any questions or concerns should be brought to the notice of Head (IT).

Application Security Policy :

1.1 Introduction

With procured developed applications essential for the very functioning of the McDonald's, they must be protected with various security controls. Application software without appropriate authentication, input, processing and output controls could be vulnerable to attacks. This policy mandates that the applications deployed in the McDonald's production environment are tested and secured against latest vulnerabilities.

1.2 Policy Statement:

Applications deployed in the McDonald's must have controls for secure input, processing, storage and output of data. Applications must be tested for security and performance before deployment and must be managed for high availability. Access to application must be restricted to authorized persons and access be provided on the principle of least privilege.

1.3 Scope

This policy applies to:

- All applications being developed procured / outsourced to third vendors.

1.4 Standards and Procedures

1.4.1 Application Access

The application must have effective in-built authentication and privilege management facilities including but not limited to the following:

- Application must authenticate all users before allowing access.
- Application must have the provision for allocating access rights based on the principle of least privilege.
- Role based access controls must be defined. The access level for the roles must be documented by the Application owner.
- The application must restrict menu options based on a need to know and need to do basis according to user roles.

- Access must be granted through User Access Request form –application only after the authorization by the Operations/ Business / Department Head.
- New user creation and privilege granting must be done by different persons.
- There must be a facility for provisioning multiple privilege levels based on business and functional requirements.
- Unique user IDs must be created for provision of application access. User IDs must not be shared between individuals for access to any application.

Application must ensure that all transactions have a separate requestor and approver. No individual irrespective of his grade, title or function will complete a transaction involving sensitive, valuable, or critical information from initiation to the final authorization.

Application must enforce appropriate logon information. Details regarding the date and time of last successful/unsuccessful logon must be displayed.

1.4.2 Data Security

User login passwords must be stored in an encrypted format. The user passwords must be stored in such a way that it is not retrievable even by system administrators / application developer.

Application server must be secured as per the corresponding Secure Configuration Document.

1.4.3 Performance Testing

Application owner must ensure that application is tested for peak load conditions before deployment. For all multi-user applications, the load testing needs to be done in environments which simulate real life conditions.

1.4.4 Security Testing

Application must be subjected to security testing under the following scenarios:

- There is a major software change including version upgrade.
- There is a major functional change in the application.

1.4.5 Account Policy

Application must enforce stringent password policies in alignment with the Password Policy of the McDonald's.

- Application must enforce minimum password length of 8 characters.
- Password expiry must be set to a period of 30 days.
- Password history must be set to 5 passwords. The last 5 passwords must not be re-used.
- Application must force a new user to change the password at first logon.
- Application must enforce appropriate lockout duration for accounts and timeout duration for sessions.
- The application must lock the user account after 5 successive unsuccessful login attempts

- For applications made available for the customers over the Internet, the application must force the user to use "forgot password" feature after the user account is locked.
- Application must initiate a session timeout after 10 minutes of inactivity and must force the user to enter the password for gaining access.

User accounts that are part of the default installation of the application, but are not required for normal operations must be disabled.

1.4.6 Audit Logs - Creation and Monitoring

The application must have the facility to log all transactions and security related events including the following:

- User account management
- User Privilege changes
- User login/logout time
- Changes in application configuration
- Authentication failures

Efficient mechanism must be implemented for monitoring and reviewing of the logs, based on the criticality of the application.

Application owner must define the retention period for the logs after considering relevant regulatory, statutory and audit requirements.

1.4.7 Additional Controls for Web Applications

Web applications must be secured against the following key vulnerabilities:

- **Broken session management:** This vulnerability arises due to improper protection of account credentials and session tokens. This could lead to attacks that can compromise passwords and session cookies and bypass authentication restrictions.
- **Cross-Site Scripting (XSS) flaws:** This vulnerability can result in the web application being used as a mechanism to transport an attack to an end user's browser. It can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
- **Buffer overflows:** Web application components that do not properly validate input can be crashed and, in some cases, used to take control of a process.
- **Command injection flaws:** Web applications pass parameters when they access external systems or the local operating system. If malicious commands are embedded in these parameters, the external system may execute those commands on behalf of the web application.

1.4.8 Change Management

All changes to the application must be as per the Change Management Policy. The changes made to the application must be documented and maintained in addition to the existing application documentation.

1.4.9 Capacity Planning

Application owner must identify the system requirements for deploying the application. This must include the following but is not limited to:

- Hardware requirements like processors, hard disk capacity.
- Software requirements like supporting OS and application software
- Bandwidth requirements

The current needs and future requirements must be considered while determining the above specifications.

1.4.10 Firewall

All critical applications must be placed behind a firewall to segregate from internal and external users.

Application owner must consult with Information Technology Department to determine the need for protecting the application servers behind the firewall.

Application owner must approve the request for firewall rule base pertaining to the application (IP addresses, Ports and users) and forward the same to IT Administrator for implementation.

1.4.11 Documentation

Application owner is responsible for creating the secure configuration document. This must cover all security settings as specified in the application security policy.

Application owner must ensure that detailed documentation is available for the following activities:

- Application installation
- Configuration settings
- Privilege levels and associated staff categories
- User Procedures
- Backup and recovery procedure
- Data retention period

All settings mentioned in the secure configuration document must be incorporated in the application documentation. Adequate backups of all documentation must be maintained.

1.4.12 User Access Review :

1. Privileges assigned to application user should be reviewed once in 6 months.
2. The HOD of the user must approve the list of users in his department.
3. For Store users, Manager of Restaurant Manager review list of userID and should approves the same
4. All User ID's above Restaurant Manager level in operations should be reviewed and approved by the Regional Director of the respective region. Subsequently, IT Manager must approves the Access Review form.

1.4.13 User Access/ID Creation :

1. The HOD of the user should submit request for User ID creation through User Access Creation Form. Along with approval.
2. The privileges to be assigned to the User ID would be mentioned in the form
3. The same must be approved by HOD, subsequently by IT-Manager/HOD.
4. For User ID at store level, a mail with the approval of Manager of Restaurant Manager is a must.
5. For User ID at store level, the mail request must be subsequently authorized by I.T Manager/HOD
6. For all User ID in operations above Restaurant Manager level, request for the User Access Creation must be approved by Regional Director of respective region.

1.4.14 User Access/ID Disabling:

1. Exit form of the separated Employee would list the application name and user id that need to be disabled. The same should be approved by users HOD.
2. In case of User ID at store level, the ID's should get disabled through User Access Review process.

Change Management:

Introduction

Unauthorized changes and unstructured implementation of information assets can lead to system downtime and cause denial of service to users who need access to the system. The aim of change Management is to maintain service stability by ensuring that changes go through the correct level of documentation, review and approval before they are implemented on McDonald's IT infrastructure and applications.

Policy Statement

Changes to information assets must be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level.

Scope

This policy applies to:

- All IT assets of the McDonald's.

Personnel covered by this document include:

- All IT personnel administering and maintaining the IT infrastructure.
- All personnel responsible for approving and tracking changes
- All business or application owners responsible for the smooth functioning of the assigned IT assets.
- All IT personnel responsible for carrying out the approved changes.

Standards and Procedures

Change Request and Approval

All changes to the IT infrastructure must be preceded by a change request.

The change request must contain the following details:

- **Change objective:** There must be clear justification for change. This could include new business requirements, product feature enhancements and problem rectification.

Categorization of the change: The change requested should be categorized in 4

Categories: 1) Major 2) Minor 3) Emergency 4) Bugs

- **Major Change** : Any change that affects coding of the application, which affects business logic in the application is a major change. Eg : change in process of calculating attendance or payroll, change in capturing consumption of raw materials. etc

- **Minor Change** : Any change that does not affect coding of the application, which does not affect business logic in the application is a minor change. Eg : change in color of screen, or design of the screen etc.
- **Emergency changes :** are those changes which need to be carried/done immediately to avoid outage of application/system/Infrastructure.
- **Bugs :** System does not work as expected or designed, it is referred as bug.

- **Description of the change:** The details regarding the changes including configuration changes, installation of additional components and system restart requirements must be documented.
- **Alternative solution:** If there are alternative solutions, which could achieve the same benefits, these must be documented.

1.4.1.3 Approvals :

All changes must be approved as below :

Major Change

Application/System	1st Approval	2nd Approval
Application	Head of Department	IT-Manager/Head
Financial System	Finance Manager	IT-Manager/Head
Infrastructure /Hardware	Head of Department	IT-Manager/Head
Password/Security policies		IT-Manager/Head

Minor Change

Application/System	1st Approval	
Application	Head of Department	
Financial System	Finance Manager	

Emergency Change

Application/System	1st Approval	2nd Approval
Application	Head of Department	IT-Manager/Head
Financial System	Finance Manager	IT-Manager/Head
Infrastructure	Head of Department	IT-Manager/Head

Change Implementation Plan

The team responsible for implementing the change must develop a detailed implementation plan that includes the following details:

STEPS

- **Time and resource requirements -** The time and resource (in terms of people or additional software/hardware) requirements for implementing the change must be documented.
- **Pre-requisites -** If there are pre-requisites including completion of day end activities or taking a full backup that need to be met before the change can be done, these must be documented.
- **Downtime requirements –** If the change involves system downtime, then it must be scheduled during non-business hours. Arrangements must be made for availability of system personnel and specific users needed to implement and verify the change. The information on the downtimes must be circulated to the concerned stake-holders including the ISG(Information Security Group).
- **Implementation steps -** The steps that need to be executed to implement the change and the personnel responsible for executing the steps must be documented in detail, ensuring the segregation of duties.
- **Test plan –** The procedure for testing the change must be documented. The team responsible for implementing the change needs to consult with end-users while creating the test plan.
- **Rollback plan –** There must be a documented roll back plan for restoring the system to original state. The time and resources required to implement the rollback plan also must be documented.

Application owner must evaluate the implementation plan for completeness and operational feasibility before approval.
In case of Major Changes all 6 implantation step to be followed and in case of Minor, Bugs and for emergency changes only Step1 and Step 5 must be followed.

Change Testing

The change must be initially tested on a non-production system. For changes in software application code, the change can be tested on the staging / UAT server. The changes must be made on the staging system as per the implementation plan. Testing must be done to verify the changes.

Implementation of Change

The team responsible for implementing the change must follow the plan approved by the application owner. The test plan must be executed and sign off obtained from teams involved with testing.

The implementation team must submit a post implementation report to the application owner. This must include the following details

- Time and resources
- Implementation steps involved
- Test plan results
- Justifications for deviation (if any) from plan

Emergency Changes

Emergency changes (e.g. system, breakdown, priority security patches etc.) must be carried out only under exceptional circumstances. Such changes must be carried out as necessary on receiving verbal approvals from the requester HOD.

The following steps must be taken to ensure integrity of the computer systems during such situations:

- The emergency changes must be allowed only to resolve production problems.
- Application and business owners must document the approved changes and report them to the IT Head.

The team responsible for implementing these changes must have an implementation plan with roll back facility.

The team responsible for implementing the change must submit a post implementation report to application owner. This must include all details of the change including the following:

- Reason for change
- Implementation steps involved
- Test plan results

Review of Change

On completion of implementation the effectiveness of change (including minor/emergency changes) must be evaluated by the IT Team Head. The following areas must be considered:

- **Changes achieving the desired objective:** IT Team Head must evaluate if the objectives defined in original change request have been met. This can be done by taking feedback from system administrators and users.
- **Adherence to implementation plan:** IT Team Head must evaluate if all the steps that were proposed in the implementation plan have been followed and if the time and effort estimates were appropriate.

If the changes do not meet desired objective, IT Team Head must inform the implementation team to roll back the change

All the changes in the IT assets must be tracked and reported and must be available to the IT Head and the CISO for review

Incident Management

Introduction

The term 'incident' can be defined as any irregular or adverse event, which occurs on any part of the McDonald's information systems. Incident management responsibilities and processes must be clearly defined. This would help to minimize the damage from security incidents and malfunctions and help to monitor and learn from security incidents. This policy is intended to establish, communicate and implement formal methods and procedures for detecting, reporting and managing events and incidents relating to exceptional situations involving security of information.

Policy Statement

All security breaches or attempts to breach and all discovered security weaknesses in information systems must be reported. Incident management process must ensure that all reported security breaches or weaknesses are responded to promptly and action taken to stop reoccurrence.

Scope

This policy applies to:

- All information assets of the McDonald's
- All employees and
- All third party personnel accessing the McDonald's IT resources

Standards and Procedures

Incident Identification

The Information Security Group (ISG) along with the nominated members of any other team/Individual/Stakeholder forms the Incident Management Team.

An incident is defined as an event or act of violating an explicit or implied security policy or information security safeguard implemented by the McDonald's. The following actions can be classified as incidents:

- Attempts to gain unauthorized access to a system or its data, masquerading, or spoofing as authorized users
- Unwanted disruption or denial or service
- Failure / Crash of IT Equipment
- Hardware resources and components lost/stolen
- Major Virus incidents resulting in Business loss or downtime.
- Natural Calamity or disaster
- The unauthorized use of a system for the processing or storage of data by authorized users

- Changes to the system hardware, firmware or software and data without the owner's knowledge, instruction or consent
- Existence of stray user accounts
- Theft of / Damage to computer hardware equipment or communication network.
- Information system failure and loss of service
- Loss of Information related to payment processing data

All users and administrators are responsible for identifying incidents and informing the IT Helpdesk for ensuing action. A few pointers that could help the concerned parties identify incidents are as follows:

- **Abnormal system resource usage:** If the CPU or memory utilization on a system is very high compared to the normal usage in the past, the system could have been compromised. Compromised systems could be exploited by attackers for spreading viruses or infecting other machines leading to high resource utilization. System administrators need to track resource utilization and analyze reasons for any abnormal usage.
- **Abnormal, slow response of the application:** Users could experience extremely slow response times if the application servers or the network has been compromised and is being used for malicious purposes. Virus or worm outbreaks could lead to network congestion which would in turn cause application responses to be slow and unstable. Incidents must be reported in instances where the response is extremely slow as compared to the past usage.
- **Data Corruption:** If the user finds that data or files stored on the desktop has been either deleted or modified without their knowledge, this could be an indication of a compromised system.
- **Change in desktops:** If the desktop configuration looks different in terms of the applications installed, screen savers or icons on the screen, or the system is misbehaving in terms of opening new screens without their commands, it could be an indication of their system being compromised.
- **Changes in passwords and user-id:** Users must report if they find their passwords have been changed or their account has been locked without their knowledge. Any changes in user passwords could be indications of system compromise. Users must report if they have suspicion of someone else using their account like emails sent from their mail id or applications accessed from their account or data posted from their account without their knowledge.
- **Virus infection:** Users must report any virus or worm that infected one or more hosts. However viruses or worms that are detected and cleaned by antivirus software need not be reported; only those which are not getting cleaned and infecting the system needs to be reported.
- **Changes in applications:** If the applications accessed by user look different from its normal appearances or user level of access in the application appears to have been modified (either increased access or decreased access), the application may have been compromised.

- **Security weakness detected:** If any weakness has been detected by user in the applications accessed by user that can cause unauthorized access or modification or lead to any kind of compromise, need to be reported.
- **Violation by others:** If users come across any instance of security violations committed by others like running of malicious tools, trying to break into system or committing IT frauds or thefts, copyright or license agreement violations, user must report such instances. Access to data or a system without authorization, may include but not limited to:
    - Unauthorized use of an account (privileged or otherwise)
    - Unauthorized access to directories, files or media
    - Placement of 'sniffing' hardware or software on network segment to capture data travelling across it
- Modification of data without authorization. Such attempts may include but not limited to:
    - Unauthorized movement of files
    - Trojan horse or virus code
    - Deletion of data
    - Modification of data
    - Change of file permissions
    - Web page defacement
    - Alteration of file content
- Denial of service or disruption to system activity. Such incidents include but are not limited to:
    - Distributed denial of service attack (DDoS) causing loss of external network connections through packet flooding
    - Exploitation of vulnerabilities causing network outage
    - Causing system to crash
    - Causing system to lose connectivity
    - Causing system to partially or completely fail
    - Physical loss or damage to systems
- Changes to system software/firmware, hardware or environment without approval. Such incidents include but are not limited to:
    - Installation of back door code without authorization (including violations by system developers)
    - Modification of system code without authorization
    - Modification to cabling (patching, rack connections etc.)
    - Addition of software/hardware with malicious intent (e.g. keystroke logging or backdoor)
    - Unauthorized removal, addition or replacement of equipment
- Probe/ Scans: Attempts to gain information that may be used to perpetrate an attack, including but not limited to:
    - Port scans
    - Targeted scans across whole, or large part of, IP range

  - Social engineering attacks
  - Unexpected inquiries into network capabilities/vulnerabilities
  - Unauthorized password resets
- Loss or physical damage to the systems
- Unauthorized activation of suspended / deleted user accounts
- Existence of unknown user accounts: Unknown accounts, especially those with administrative privileges, could indicate that system has been attacked.

Incident Reporting:

On suspected occurrence of a security violation, it must be reported to the IT Helpdesk.

Incident Assessment

IT helpdesk team must do a preliminary analysis of the incident before reporting it to the IT Manager. Typical information pertaining to an incident that would be reported includes but is not limited to:

- **Description of the incident:** Details regarding the logical and physical events regarding the incident, date and time of the incident and the reporting person.
- **Possible causes:** Based on the damages observed and other evidence available, system administrators must include the possible causes of the incident. This could include worm/virus attacks, password compromise or social engineering.
- **Damages observed:** All loss of data, system downtime, system instability and slow response times must be included.
- **Supporting evidence:** All evidence regarding the incident including system or application log files, alerts and logs of security devices including firewalls must be included in the report.
- **Remedial steps taken:** Any preventive measures taken like disconnecting the system from the network, changing administrative passwords or application of new patches.

Incident Verification

IT Manager must analyze the incident based on the data received from the IT Helpdesk.

The matrix for deciding the incident priority level is as given below:

Priority Level	Nature of the Incident
Critical	Direct threat or damage to image, reputation or credibility of the McDonald's. Multiple business functional units getting severely impacted. Location of business critically affected. Business continuity measures to be invoked.
High	Severe outage affecting single business functional unit, key services or location.

Priority Level	Nature of the Incident
Medium	Moderate degradation to business functional units, locations, IT assets. Moderate to high impact to non-critical business units within the McDonald's.
Low	Small issue with localized scope that can be tolerated for a finite period of time. Affecting few resources.

IT Helpdesk must record the incident and allocate an incident number for tracking and record the same in the incident tracking register.

Based on the information available and the identified level of the incident's criticality, IT Helpdesk must send incident alerts to the respective asset owner, application groups and user departments which have been affected.

Incident Recovery

Depending on the nature of the incident and based on the action plan drawn up by Incident Management Team, all system personnel and security professionals required to recover from the incident must be contacted. Recovery will involve identifying and eliminating the cause of the incident. This could involve a series of activities including but not limited to: implementing additional security controls, installation of new patches, recovery of systems backups, and reconfiguration of security devices including Firewall rule base and intrusion detection system alerts.

Post recovery, additional security monitoring devices must be configured to ensure that the incident activity has ceased. This could involve a series of activities including deployment of additional intrusion detection systems, frequent monitoring of system and application logs of affected systems.

Incident Prevention

Based on the learning from the incident, the IT Manager must make recommendations to the IT Application owner for procuring additional security services and solutions (if required) for improving security.

IT Helpdesk must maintain a database of incidents and solutions. This will help in providing quicker solution if the same or similar incident repeats.

Incident Register

Logging of information on the security incidents must be maintained and updated. The information must be logged with appropriate access controls and responsibilities for maintenance

Escalation Matrix :

Level	Name	Area	Email ID	Contact No
Level 1	ITsupport Central	All	itsupport.central@mcdonaldsindia.com	022 6734 7373
Level 2	Rahul Jiman	West Stores	rahul.jiman@mcdonaldsindia.com	9892956114
Level 3	Samir Raut	South Stores	southops@mcdonaldsindia.com	9821836821
Level 4	Tanaji chaudhari	Infra	tanaji.chaudhari@mcdonaldsindia.com	8879770402
Level 5	Parvez Khan	POS related	Parvez.khan@mcdonaldsindia.com	8879885521
Level 6	Anand Tomar	All	Anand Tomar@mcdonaldsindia.com	9594940301

Enforcement

Compliance with the security policies will be a matter for periodic review by the Information Technology Department. Any employee found to have violated this policy may be subject to disciplinary action, up to termination of employment as deemed appropriate by the policies of management and human resources.

_____ *End of Document* _____