The Dharamsi Morarji Chemical Co. Ltd.

INFORMATION TECHNOLOGY POLICY

Company Confidential & Internal Use Only

IT Department

Document Controls

Version No.	Date	Author	Document Name	Approval
1.0	31.05.2020	IT Dept.& Mahajan & Aibara	Initial Document	Ramchandra Warang (Chief – IT & Systems)

Contents

Introduction

The Dharamsi Morarji Chemical Co. Ltd (DMCC) Information Technology Policy is based on the following principles:

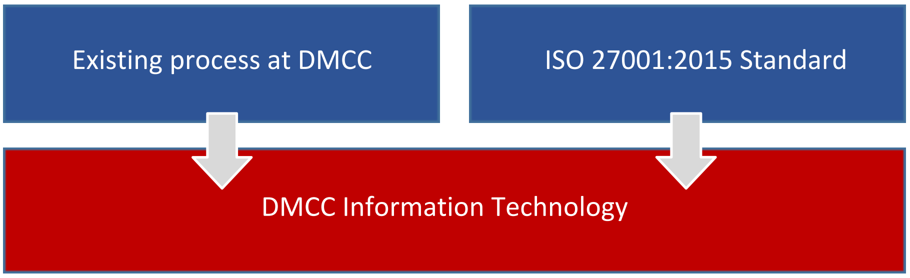
- **Confidentiality:** Protection of information by ensuring that information is accessible only to those authorized.
- **Integrity:** Assuring accuracy and completeness of information and its associated information processing methods.
- **Availability:** Ensuring that information and associated assets or systems are available to authorized users when required.

The overall objective of DMCC, towards Information Security is:

- To ensure the protection of DMCC assets and information against damage or destruction and unauthorized disclosure or changes, whether it is accidental or deliberate.
- DMCC information systems shall comply with relevant laws and regulations.
- To ensure accountability of user actions carried out using information systems.
- To raise awareness about the security risks associated with information and information systems among its employees.
- To implement mechanisms to ensure that all breaches of information security and suspected weaknesses, are reported and investigated, and followed by adequate action.
- To implement sufficient controls to minimize loss of DMCC information, data and other resources due to fraudulent activities.

Policy Brief

The policy document is formulated by assessing the existing processes at DMCC while referring the ISO27001:2013 standard. The DMCC information technology policy includes aspects of security related to logical access management, password management, e-mail management, IT asset management, change management, data backup, retention and restoration, network security and industry best practices.
This policy is applicable to all IT assets, comprising computer systems, being used at DMCC for supporting critical business functions and people associated with it, which hereinafter is referred to as Critical Information Infrastructure (CII) in this document.
In Information Technology Act 2000, Critical Information Infrastructure has been defined as: "Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which shall be debilitating impact on national security, economy, public health or safety."



Existing process at DMCC

ISO 27001:2015 Standard

DMCC Information Technology

Responsibility and Accountability

All employees, external contractors, and other third parties, who access DMCC information systems, are responsible for ensuring that information security policies of DMCC are adhered to, and that they operate systems in such a manner as to ensure its security. All users are accountable for actions carried out by them on information systems. Management at all levels is responsible and accountable for ensuring that staff are aware of, and adhere to this policy. It is the responsibility of Head of IT to ensure that the approach outlined within this framework is implemented.

Updating and Distribution of the Policy Document

Any major change in policy would be initiated by Head of IT and incorporated only after approval of the DMCC management committee. The Head of IT shall be responsible in communicating the same to all service providers and employees or parties who may be directly or indirectly impacted by the change in policy.

This policy must be reviewed at least once a year and changes to policy and standards must be identified. The policy must be updated based on the outcome of this review. Every person in custody of this document has the responsibility for ensuring its confidentiality. The owner of this document is the Head of IT and shall ensure that the document is continually updated with amendments that may be issued from time to time.

Logical Access Management Policy

Objective

- The purpose of this policy is to define required logical access control measures to all DMCC’s information systems in order to ensure the confidentiality, availability and integrity of those assets.
- This policy also entails managing the life-cycle of access control including provisioning and de-provisioning processes.

Scope

- This policy is applicable to all users who require access to any DMCC information asset irrespective of business unit location / geographical location.
- The scope of this policy extends to managing the information security risks related to logical access controls to information and information systems, inclusive of, but not limited to:
  - Applications like SAP Business One, Payroll, TALLY, etc.
  - Databases
  - Operating systems
  - Computing systems
  - DMCC Networks and networking devices
  - General user accounts, privileged user accounts and shared accounts (e.g. service / system accounts)
- The procedures shall be administered to ensure that the appropriate level of access control is applied to protect the information in each application or system from unauthorized access, modification, disclosure or destruction to ensure that information remains accurate, confidential, and is available when required.

Policy Statement

- This policy intends to communicate the access control policy for access to information systems inside DMCC, based on business requirements.

A. *Access Management*

1. Access shall be provided to information and various information processing facilities for the employees of DMCC and "third party personnel " (contract employees, subcontractors and vendors) upon completion of the access request / granting formalities. The information processing facilities include, but not limited to, desktops, laptops, applications, active directory/domain, network devices, servers and mobile devices including tablet computers.
2. Access to DMCC systems shall be restricted only to DMCC's employees and third party personnel.
3. Access to the information and information systems shall be controlled on the basis of business and security requirements. Access controls shall be deployed to protect information from unauthorized access.

B. *User Access Provisioning*

1. DMCC users should be granted access to information, data and applications strictly on a "need to know" basis. A new user (employee) may request for access to the specific application by raising a request using ‘New System Request form’ to the IT department. The request should capture the following details:
   - Employee name
   - Employee ID

- Department and name of the respective HOD providing the approval
- List of application(s) to which access is required
- Business justification for the requirement of access to the specified application(s)
- Contact Information

2. The user is granted access rights to domain, applications and data after the request is scrutinized and approved by the respective department/functional HOD, systems in-charge and the Head of IT. The request will only be approved if both the approvers are satisfied with the business justification provided.
3. Access to information services should be controlled by using unique user IDs, wherever possible, to ensure accountability of individual users for his/her activities/actions.
4. Generic IDs should not be provided to users. In exceptional circumstances when a generic ID is created, it should be tied back to a unique user, who would be nominated by the department HOD to take ownership of all responsibilities for actions performed by the ID. Generic or shared IDs are generally created for a specific department or function. All generic IDs and their corresponding user mapping should be documented along with appropriate justification and approvals and retained for audit purposes.
5. Contract employees and other external support users may also be granted access to the DMCC systems or applications based on the business requirements, and the process followed would be the same as above. However, the access would be created, only once HR and respective HODs intimates the IT team about the addition of a new contract employee.

C. *User Access Modification*

1. If for any reason, a user’s access rights need to be modified in an application, the respective department HOD should send an intimation by e-mail using ‘New System Request form’ to the IT department and Head of IT, specifying the reason for the modification.
2. All user modification requests will be through email and follow the same approval flow as access provisioning procedure. The users should also specify whether they would require their existing access rights while raising the modification request.
3. If the existing access rights are no longer required, the same should be revoked prior to granting the modified access.

D. *User Access Revocation*

1. On the last working day of the employee, the HR team will send an intimation by e-mail using ‘New System Request form’ to the IT department and Head of IT, as part of the exit formalities, updating with the necessary details. This is done to ensure there is an audit trail of all access revocation requests.
2. Once the access revocation intimation, the system in-charge receives an intimation about the exit of the employee.
3. The access of the resigned employee to the information systems is disabled/deactivated on the last working day of the employee.
4. For contract employees, the HR/Functional HOD would intimate the system in-charge regarding the exit, via an e-mail. The remainder of the process followed for access revocation will be the same as the process followed for DMCC’s employees.
5. For other external support users, the Functional HOD would intimate the system in-charge regarding the exit, via an e-mail. The remainder of the process followed for access revocation will be the same as the process followed for DMCC’s employees.

E. *User Password Management*

1. A strong password is the key defense against any attempt to compromise the logical security of information systems.
2. Weak passwords increase the vulnerability of information systems to brute force and/ or dictionary attacks.
3. All users of information systems shall have the responsibility to ensure that strong passwords are chosen for the information systems.
4. The guidelines for creating, maintaining, protecting and deleting passwords are mentioned in detail in the DMCC's ***Password Policy.***

F. *Privilege Access Management*

1. Privileged access includes providing elevated access rights to users for applications, domain, servers, database, network devices and operating systems.
2. Privileged access would be provided to authorized users based on their job role, along with the recommendation and approval from the respective department HOD, system in-charge and Head of IT. Privileged user access shall be restricted to a minimum number of users based on valid business need and reason.
3. Each administrator should be assigned his/her own unique administrator ID (domain/server/ application/database/network device) to ensure accountability. Administrator IDs will be assigned the necessary administrative capabilities so that the user may carry out his/her assigned job functions.
4. Sharing of administrator accounts is not permitted, unless an exceptional approval is obtained from the Head of IT after specifying a valid business justification.
5. In order to ensure segregation of duties, administrative privileges should not be assigned to an individual user ID.

G. *User Access Review*

1. Reviews of Access Rights: The review of access rights associated with generic user accounts in each application should be performed on a half-yearly basis. The systems in-charge should compile a department/function wise list of all active user IDs, capturing the following details, but not limited to, user ID, current access and privilege levels, the number of days since last accessed, etc. This list should be forwarded to the respective department/function HOD. The function/department HOD should verify the continued need for all access rights granted. The systems in charge should modify the access rights based on the review comments and feedback from the respective HOD.
2. Review of Privileged Access: The Head of IT should review and verify the continued need for use of all privileged operations granted in the IT environment. All changes made to the privilege accounts should be documented and approved. The review of access rights to privileged accounts should be done on a half-yearly basis by the Head of IT.

H. *Exceptions*

1. Any exception to the policy must be formally approved by the IT Head and HOD.

Password Policy

Objective

- The objective of this policy is to establish criteria for provision of passwords and conditions relating to their use.

Scope

- The password policy set out in this document are applicable to all users at DMCC who have access to any of the system, applications and network devices at DMCC.

Policy Statement

- This policy intends to communicate the access control policy for access to information systems inside DMCC, based on business requirements.

A. User Responsibility

1. The users of all systems are responsible for ensuring that his/her passwords are kept confidential to prevent unauthorized access to any of the DMCC systems and to maintain the confidentiality of information held on the systems.
2. Users shall not write down his/her passwords. Sharing of passwords (except for shared User IDs) is not permitted without appropriate approvals from the respective functional HODs.
3. Where the system permits, the users must be forced to change the password at first log-on. Additionally, any password change must be permitted only after successful authentication.
4. Password must never be displayed in clear text or stored in readable form in batch files, automatic login scripts and terminal functions keys or in other locations where unauthorized people might discover them.
5. Where it is necessary to write down a password for contingency reasons e.g. administrator passwords, they should be put in a sealed envelope and place them in a safe, maintained by the Head of IT.
6. For passwords to be an effective security measure, users should make sure that the passwords are complex and may not be easily retrieved by other users. Users should make sure that his/her passwords meet the minimum requirements as specified under ***Section B (Password Specifications).***
7. Initial Passwords: When the system administrator creates user accounts, a unique initial password (only if the system/application permits) would be assigned and the same would be communicated to the user in a more secure manner. The initial password should not be the same as the user ID. The system or application or network device should provide a means of requiring the user to change the initial password (only if the system/application permits) upon initial logon.
8. Changing Passwords: The system administrator should have the appropriate access rights to change a password associated with a user account. If the system administrator changes a password, the system would treat it as an initial password (only if the system/application permits). When a user changes a password, the user would be required to enter the current (or previous) password, after which he would have to enter the new password. Password change should require the user to confirm the new password by re-entering the value and the two values should precisely match for the change to occur.
9. When passwords associated with generic accounts are changed, it would be the responsibility of the user – who was nominated to take ownership of the generic ID – to change the password and to securely communicate the new password to all members of the group of users for the account. Members should be cautioned not to change the password when logging onto the generic account, but instead, should notify the nominated user that a change is required.

B. *User Responsibility*

1. DMCC should ensure that all systems meet the following minimum password complexity requirements, to the extent possible:
    - The password must contain a minimum of 8 characters.
    - The password must contain at least one alphabet, a-z, A-Z.
    - The password must contain at least one numeral, 0-9.
    - The password must contain at least one special character,~,!,@,#,$, %,^,&,*,(,).

C. *Exceptions*

1. Any exception to the policy must be approved by the IT Head and HOD

Data Backup, Retention and Restoration Policy

Objective

- This policy is established to define the requisite controls around data backup and recovery in order to reduce the risks attributed to loss of DMCC's critical data.
- The scope of this policy on data backup and restoration for any DMCC information systems or networks components that store critical data.
- It does not address backup and restore activities performed by DMCC employees (for backup of documents) or other third parties (including Cloud service providers) except as addressed by specific contractual agreements.

Scope

- The scope of this Data Backup, Retention and Restoration Policy is as follows:
  - Backup Schedule and Procedure
  - Maintain a backup schedule defining the scope of backups outlined in this policy.

  Offsite Tape Movement

  - Controls to ensure that the critical data, identified by DMCC, is securely stored away in an adequately controlled safe location which is away from the primary location of data center.

  Backup Restoration Procedures

  - Backup controls to ensure the integrity and availability of critical data so that they can be restored in line with the business requirements.

Policy Statement

A. Backup Schedule and Procedures

i. Backup Schedule

1. The technical team shall be responsible for maintaining and updating the backup schedule document, which defines the frequency of all backups taken at DMCC.
2. Critical data and operations should be identified, documented, prioritized, and approved by the business process owners, in cooperation with IT management. It shall be ensured that all critical servers and data are captured along with the type of backup that needs to be performed. A list of what needs to be backed up shall be documented as well.
3. The backup schedule shall mention the date / time and details of data that is going to be backed up. Once validated, all the technical team members responsible for taking backups should follow the schedule and take backups

   Accordingly, any non-compliance should be noted and reported to the Head of IT.

ii. Backup Procedure

1. During the regular backup routine, a technical team member shall take the backup as per the backup schedule, or on an 'on-demand' basis depending on the criticality of the data and user/activity requirement.
2. Continuous monitoring of backup is to be performed by the technical team to ensure that there are no discrepancies and all backups occur as scheduled.
3. The backup logs are to be maintained by the technical team. The log is to be reviewed on a monthly basis by the technical team and approved by the Head of IT

4. The backup tape media should be labeled for identifying the content of the tape to ensure an easier and faster restoration process. The tape media label should capture the following information, but not limited to:
   - Application name/Operating System name
   - File System/Database name/Logs
   - Full/Incremental
   - Tape number
5. A tracker should be maintained to capture the content details of each tape against the respective backed up date.
6. The retention period of backup tapes will be defined in the backup schedule document.
7. Backup of DMCC's critical data should be maintained in a NAS drive.
8. The retention period of NAS drive/backup tapes is defined in the backup schedule document.

B. *Backup Restoration Procedures*

1. Backups of critical data shall be restored in a test area every six months depending on the backup strategy to test restoration procedures and the storage on devices. The recovered data is then verified and authenticated by the owner.
2. All the backup media which were used for recovery is returned to the on-site/off-site location after the recovery testing is complete in a sealed and tamper proof envelope.
3. It is the system administrator's responsibility to ensure that the restored data is deleted after successful completion of testing.
4. Frequency for restoration testing shall be decided by the Head of IT, depending upon criticality of backup. The details for each restoration test shall be documented and recorded.

C. *Data Backup – Employee Work Data*

1. It is the responsibility of each employee to ensure that his/her work data is backed up regularly. The backup tool and the repository to store the backed up data shall be provided by the operations team.

D. *E-mail Backup*

1. As per the "IT Act 2000", email records have legal validity and can be used as evidence in the court of law. Thus all emails should be stored in a safe and confidential manner.
2. Emails older than 1 year are moved to email archive.
3. It is the system administrator's responsibility to ensure the emails can be retrieved as and when needed.

Change Management Policy

Objective

- **The objective of this document is to define the change management process followed by DMCC for the smooth and efficient handling of all application changes within the IT environment.**
- The primary objectives of the Change Management process are:
  - To ensure that changes are made with minimum disruption to the business operations.
  - To ensure that changes are consistent with business and technical plan and strategies.
  - To ensure that the required level of technical and management accountability is maintained for every change.

Scope

- The change management procedures set out in this document are applicable to all changes in IT applications at DMCC.
- The process also includes the review of the results of changes post implementation.
- Any change in the applications centrally hosted at DMCC fall under the category of application changes.

Policy Statement

A. *Change Classification*

- The change classification process examines the impact of the approved change on DMCC. The core team shall examine each change request and classify the change as defined below:

Change Classification	Description	Turnaround time
Normal Change	Planned changes that impact the business operation. Such changes would follow the entire Change Management process life cycle.	8 business days
Urgent Changes	Unplanned changes that may impact the business operation. Such changes need to be rolled out sooner (as per SLA defined) than normal changes and a justification needs to be provided as to why the changes need to be expedited. However, these changes would follow the entire Change Management process life cycle.	2 business days
Emergency Changes	The change requests that need to be implemented immediately to restore the production environment back to operational service. For every emergency change request, the changes follow the emergency change management process life cycle	4 business hours
No Impact Changes	Changes which have been determined to have no or less impact on the IT application. Such changes would follow the entire Change Management process life cycle.	4 business days

B. *Change Prioritization*

1. Change prioritization specifies the importance that a change requestor assigns to the change ticket. It only indicates the relative order in which a change request, for any classification, is processed and

closed. Changes are prioritized based on considerations such as risk, resource availability, urgency and impact. The changes may be prioritized as follows:

- High
- Medium
- Low (default)

C. *Change Procedure*

1. In order to sustain the continuous reliability of business applications, a systematic methodology is essential to manage any change to the operational applications. At a minimum, the change methodology should include the following stages:

Stage 1: Initiate

1. Employees may request for a change over email, by raising a Change Request.
2. The core team will assess the change requirement, based on which he/she will approve or reject the change request. Every application in DMCC will have a dedicated core team to assist with application support and maintenance.
3. The core team analyses the potential effect of the change on other information resources and potential cost implications, and classifies the change based on the nature and urgency of change. The functional specifications, change classification and the nature of the change are articulated and documented in the Change Request, to provide a clear understanding of the business requirements.
4. The core team will decide whether to develop the change internally at DMCC or to outsource the change to the approved support vendor, after internal discussions. Once this decision is made, a final approval on this matter will be obtained from the Head of IT. The change request is categorized as "In-house" or "Annual Maintenance Contract (AMC)" before obtaining the approval from the Head of ITs.
5. In case a change request is rejected by the core team, he/she must provide a justification in the comment section of the change ticket, as to why the change request was rejected.

Stage 2: Review and Authorize

1. Once the change request is approved by a core team, an e-mail message is sent to the functional HOD to obtain his/her approval for the corresponding change request.
2. The functional HOD has the privilege to either approve or reject the change request. If the change request is rejected, a justification must be provided. If the change request is approved, the request is forwarded to the Head of IT for approval.
3. The Head of IT has the privilege to either approve or reject the change request. If the change request is rejected, the Head of IT must provide a justification for rejection of the change request. If the change request is approved by the Head of IT, the change request would be formally considered for development/change.

Stage 3: Implement

1. All the tasks listed in the change request shall be processed and implemented by the core team/approved support vendor/development team.
2. The core team should ensure that all activities are completed within the scheduled target date. For any reason if the change could not be completed within the planned schedule, the core team shall inform the initiator.

Stage 4: Post Implementation Review

1. The implemented changes should be reviewed for successful completion to ensure that there has not been any adverse effect to the IT environment.
2. The post implementation review should be completed within two (2) weeks from the date of completing the change implementation
3. All users, significantly affected by the change, should be notified, via e-mail, of the change, wherever applicable.
4. Unsuccessful Changes: Any unsuccessful change identified during a post implementation review should be addressed. A change implemented in production could be defined as unsuccessful due to any of the following:
   - Expected results did not occur
   - Change caused an adverse impact to end users
   - Problems or incidents arose as a result of the change that led to service outage, impacting business operations.
5. The unsuccessful changes should be informed to the core team by the change initiator. A new change request should be raised to rectify the unsuccessful change and should be linked with the original change request. And such a change request need not follow the usual change management approval system.

Stage 5: Close

1. Once the post implementation review is successful after obtaining all approvals, the change ticket is closed and is tagged as 'Successful'. The core team stops tracking the change once it has been implemented and has been verified as 'Successful'.

D. *Emergency Changes*

1. Emergency changes are those changes that are identified as high impact, either on account of the number of users affected or the number of critical systems or services affected.
2. In case of service outages, changes must be implemented immediately in order to restore services and may not be subjected to the normal change procedures.
3. The change should be fully processed and documented in the system after the change has been implemented, and a written approval from Head of IT should be obtained. The lead-time for implementation of an emergency change is four (4) business hours.

Network Security Policy

Objective

- This policy defines DMCC's expectations on safeguarding its technology infrastructure and the organization's management strategy for securing information as a whole.

Scope

- This policy is applicable to all employees (DMCC and contract employees) and other external support users who access and use DMCC's information assets and services. The scope of the policy is detailed as follows:
  - Network Architecture Diagram and Documentation Approach
  - Remote Access Control Standards
  - Network Configuration Management
  - Network Logging and Access Provisioning

Policy Statement

A. Network Architecture Diagram and Documentation

1. The documentation created with respect to updated network diagrams, IP addressing, configuration of network devices and location of network devices should be maintained by the Network Security team at DMCC, in an appropriate network documentation register. At any point in time, the Network Security team should ensure that the latest network infrastructure specific changes adopted by DMCC be incorporated into the aforementioned documents.
2. The Network Security team at DMCC is responsible for installation, configuration, monitoring and maintenance of all network components along with handling access granting procedures for business specific servers.
3. Segregation:_Network zones should be defined in order to classify and subdivide the group of users and services based on considerations such as business criticality, IT health integrity, data information classification, user trust levels and business agreements. The Network Security team should be responsible for designing Virtual LANs to logically segregate networks and implement them across all zones.
4. Based on the aforementioned criteria, the following zones have been defined by DMCC:
   - De-Militarized Zone (DMZ): All DMCC business systems and server components that are to be accessed from the internet on a frequent basis by external support users and employees are placed inside this zone.
   - User Zone: All systems present in the User LAN belong to this zone and are logically segregated within the zone using Virtual LANs (VLAN) on a department specific scale. Access from one department VLAN to the other should be limited, as per the concerned department's business requirements.
   - Server Farm Zone: A two-tiered network architecture has been implemented at DMCC and this zone placed after the internal firewall, holds all internally accessible machines and servers.
5. Routing Baseline Security Guide: Routing controls should be implemented at the boundaries that have different Asset Owners and at major junctions, based on proper source and destination address-checking mechanisms. In particular, the Network Security team should ensure that the outbound connections initiated from DMCC be controlled so that source IP addresses are within the IP range of the network. The methodology used to implement routing controls should be documented and maintained by Network Security team. The following best practice pointers may be considered while creating a baseline security guide:

- Access to all of DMCC's network components, require authentication using a user ID and password.
- Routing between DMCC and a third party vendor should either be static or traverse via a mechanism that is controlled by DMCC.
- Controls to restrict the route between user-terminals and network services should be incorporated to prevent users from accessing applications or facilities that are not authorized to use.
- Firewalls and routers should be configured to convert the source IP address and TCP port number on packets to externally routable values.
- For IP network traffic addressed for delivery outside DMCC, firewall and/or router address translation capabilities should be used to hide internal IP addresses from external networks.

6. **Session Timeout Parameters:** The Network Security team should set applicable connection reset parameters for all network hardware devices present in the network. The default timeout parameter values should be reviewed and changed, on a case to case basis. Any exceptions to this, requires an approval from the Head of IT. The recommended values across both Firewalls (internal and internet-facing) and switching/routing devices is 10 minutes.
7. **Network Address Management:** The Network Security team should be responsible for ensuring that all components of DMCC's internal network are assigned unique and legal network addresses. Network addresses should be assigned based on the guidance provided by the network component installation and configuration procedures. The internal IP addressing schema should be compliant with Internet Assigned Numbers Authority's (IANA) reserved IP addresses for internal networks.

B. *Remote Access Control Standards*

1. <u>Access to Third Party Service Providers, Vendors and Consultants</u>

- Firstly, DMCC should sign a Mutually Acceptable Agreement/Contract with the third-party for providing access to them. This should include the following aspects, but is not limited to:
  a. Type of access required,
  b. Type of application that is to be used,
  c. Type of data that is to be transmitted,
  d. Encryption methodology required/used,
  e. Details on security policies applicable on the third party
  f. Legal implications of misuse of DMCC's resources.
- Prior to providing access, the aforementioned details should be provided by the third party vendor, which then should be approved by the Head of IT. Once approvals are obtained, the access is provided by the Network Security team. The Head of IT should analyze the impact to the security architecture before approving such external access.
- DMCC should provide remote access privileges to external vendors so as to gain authorized access to its information systems to conduct, configuration parameter alterations and/or maintenance activities.
- External vendors and/or consultants may access application servers placed inside the DMZ with their respective user credentials, through the server's public IP address. The HTTP protocol's secure version (HTTPS) should be configured to access web server applications on publicly hosted IP addresses, from end-user workstations.
- Access requirements for external parties should be provided only after receiving required approvals from the Head of IT. The Network Security team amends the required Access Control List (ACL) rules to allow access to the requested IP addresses.

- The Network Security team should conduct a risk assessment to identify the key risks involved in providing access to third parties, once in three months. The risks identified should be documented and the respective mitigating controls should be put in place to eliminate possible threats resulting out of this exercise.
- The Network Security team should maintain a record of all such external access requests processed and rights granted, along with the user accounts and monitor the connections made by the external accounts on a continuous basis. They should also periodically review the user rights provided to the business process owners, to ensure that these rights are being utilized. If external vendors are not using their respective accounts, then the Network Security team should check its validity and disable their access immediately.

2. <u>Access to Employees</u>

- The technical team require remote access to network components and other servers on the network during non-business hours. This is predominantly to monitor backup schedule status and processes, and all other maintenance activities that has to be performed during non-business hours.
- The Virtual Private Network (VPN) Connection established between the users present at a remote site with the organization's network should be encrypted using the SSL/IPsec mechanism.

C. Network Configuration Management

1. <u>Firewall Configuration Management</u>

- Firewalls are an integral part of DMCC's defense-in-depth strategy. At the perimeter, they prevent malicious traffic and attackers from entering the corporate network; while internally they help to control access on a need-to-know and need-to-do basis. The following are guidelines that are to be followed to securely manage firewalls in DMCC's network:

  a. The firewall should be primarily used for the purpose of access control only.

  b. The operating system and the firewall application should be secured based on the baseline configuration document prepared for both, the internal firewall and the external firewall/Unified Threat Management (UTM) Box. It is mandatory that all configuration settings listed in the baseline document are applied to the firewall, prior to a production release.

  c. A rule-based document should be defined and approved by the functional owner and Manager – Systems, prior to deployment. The Managers should possess a copy of the tested rule-base pertaining to the application, from the respective application administrators. This will ensure that application administrators are aware of the services that will be allowed through the firewall, prior to deployment.

  d. Both, the internal firewall and the external Firewall/Unified Threat Management (UTM) box, should not have any additional services running, that can be accessed remotely. Any unnecessary services running on the firewall would present the attackers with an opportunity to compromise the firewall by exploiting vulnerabilities associated with that service.

  e. The internal firewall and the external Firewall/Unified Threat Management (UTM) box present in this network should at all times, be configured in High Availability (HA) mode.

  f. A two tiered architecture should be implemented with the User LAN workstations present in the User zone, all internal servers in the server farm zone and all externally accessible web servers placed in the DMZ area.

  g. By default, the firewall should have a "deny-all" policy, with access granted on a need to know basis. The firewall should have a rule to deny all access that is not explicitly allowed. DMCC's Firewall rule-base should restrict access to required ports on all target machines. The source field in the rule-base should be restricted to specific IP addresses/Subnet addresses, wherever feasible.

h. At DMCC, firewall logs and audit trails recording should be scheduled on a daily basis and archived for a period of three months to meet statutory requirements and for forensic analysis.

2. **Other Network Components Configuration Management**

- The Network Security team should develop and maintain Minimum Baseline Security standards (MBSS) for all network components (Routers, Firewalls, Routers, Modems, etc.) present inside DMCC's extensive network infrastructure and should also review the compliance of configuration parameters set on all of these network devices against their respective MBSS guidelines on a periodic basis.
- The Network Security team should be responsible for monitoring network utilization, forecasting future requirements, and communicating forecasts to the Head of IT, who should ensure the adequate availability of network services.
- All external hardwired communication lines (e.g., network lines, telephone lines, etc.) should be catalogued and uniquely identifiable to the system being accessed to facilitate maintenance and security. All the lines along with its capacity should be documented and maintained by the Network Security team.

D. *Anti-Virus and Anti-Malware Management*

1. Malicious software, commonly known as malware, is software created with the sole purpose of harming and damaging information assets. DMCC uses Antivirus products from leading vendors'. Currently one for all their internal servers and another one, for all other workstations. The following minimum baseline requirements should be followed;

- The anti-virus software should be operated in real time on all servers and client work-stations and be configured for real time protection.
- The anti-virus library definitions for both products should be updated on a daily basis and weekly scans should be performed on all user controlled workstations and servers.
- In addition to having the aforementioned security products, the e-mail server should include an additional e-mail security service enabled which will be used to scan all e-mail (incoming and outbound) for viruses and/or malware. In addition, the scanner should also be capable of handling a schedule that can scan all stored e-mail once per week, for additional virus and/or malware threats.
- Downloading software from the Internet onto DMCC's information assets should be strictly forbidden unless such software products have been approved and deemed safe by the Manager - Systems.
- External media such as portable storage devices, and other devices that connect via USB ports should be strictly prohibited. The anti-virus product deployed on all end-user stations provide a feature to block the usage of such devices and this should be incorporated into the network infrastructure's operational strategy and should also be maintained throughout, by the technical team.

E. *Network Vulnerability Assessment and Management*

1. Vulnerability Assessment and Penetration Testing activities on the IT infrastructure components in DMCC's network should be performed by Network Security team on a periodic basis, to test for known software version flaws and weaknesses. It is important to verify that all known software flaws are addressed adequately. Appropriate action should be taken, as and when vulnerabilities are identified during the assessment.
2. The Network Security team should periodically review open ports and services running on them. Unnecessary ports and services running on servers, should be identified and eliminated.

3. The Network Security team should prepare a comprehensive list of assets on which the assessment should be carried out. The team should also prepare an ongoing assessment plan for all these identified assets and drive the execution of this exercise as planned.
4. The Network Security team should ensure that only proven and tested tools and/or techniques are used for vulnerability assessment and penetration testing exercises.
5. A third-party specialist should be brought in on an annual basis to perform an independent network assessment to provide reasonable assurance to the management, customers, shareholders and other stakeholders, on DMCC's current security posture. The same may be done in order to meet any regulatory or compliance requirements. On an annual basis, a detailed assessment report should be submitted to the Head of IT.

F. *Network Logging and Access Provisioning*

1. Internet Service Access Request

- Every DMCC employee who would require Internet Access to specific websites for certain specialized requirements, should raise a request using 'New System Request form' to the IT department and Head of IT, and give reasons for the requirement and the sites that he /she is likely to visit.
- This request should then be forwarded to the specific functional team's HOD and Head of IT for authorization.
- Once the authorization has been obtained, the Network Security team should provide access to the requested websites. Access to certain websites would be provided only for a definite time period which would be mentioned in the ticket and therefore, the Network Security team should keep a track of this so that access revocation for such requests can be performed in a timely manner.
- The Network Security team should be informed of any additions/transfers of individuals, so that access requirements can be reviewed and facilitated based on the new requirement.

2. Log Management

- The Network Security team should ensure that audit logging is enabled on all network components and that a review of the same be performed on a weekly basis.

Domain Policy

Objective

- The Objective of this policy is to provide guidelines on Domain in DMCC infrastructure. The purpose of this policy is to establish a standard for allocation / modification and revocation of user access to DMCC's ICT systems.
  - Capacity management
  - System acceptance
  - Monitoring system use
  - Clock Synchronization
  - User password management
  - Control of operational software
  - Password Policy
  - Log Management

Scope

- This policy is applicable to all individuals or Systems / Equipment's in the DMCC Infrastructure.
- This policy is for use by people who access the Systems / Equipment's at DMCC.

Policy Statement

- All Systems/ Equipment's must be added in DMCC Domain. All below mentioned policies are deployed through a centralized domain controller.

A. *Password Policy*

1. **For Windows Users**
   - Password length: - Minimum 8 characters.
   - Complexity Password: - Yes
   - Minimum Age: - 180 Days
   - Maximum Age: - 181 Days
   - Password History: - 5
2. **For Windows Server Users**
   - Password length: - Minimum 8 characters.
   - Complexity Password: - Yes
   - Minimum Age: - 90 Days
   - Maximum Age: - 91 Days
   - Password History: - 5
3. **Account Lockout Policy**
   - Account Lockout Duration: - 30 Minutes
   - Account Lockout Threshold: - 5 invalid login attempts
   - Reset Account Lockout Counter After: - 30 Minutes

B. Desktop and Screen Saver Policy

1. Same wallpaper applies on all system.
2. IMS. screen this screen saver applies after 4 minutes' waits.

C. Proxy Policy

1. Prohibited to change Proxy setting by domain users.

D. Network Card Policy

1. Prohibited to change IP address by domain users.

E. Windows Update Policy

1. All the systems are updated by using WSUS in the same forest.

F. Removable Mass Storage Policy

1. Prohibited all Removable storage (e.g. Pen Drive, Memory Card, Mobile, etc.)

G. IIS Policy

1. Domain users can manage IIS manager in the server.

H. Clock Synchronization

1. Domain users clock timing is pushed from Domain Controller.

I. Installation Policy

1. All default software available for Installation on every system in Control Panel.

J. Multiple DC

1. All the users are connected with their respective location domain controller.
2. All domain controllers replicate all objects and policies to each other between our two offices.
3. If any respective location domain controller goes down, then automatically all users will shift to the additional domain controller OR
4. If respective location both domain controllers not accessible at that time all users will connected to other respective location domain controller.

K. Eligibility for adding Domain control

1. All employees of DMCC & consultants are eligible for domain connection default as "Normal" domain connection. Prospective special users shall put a request through an Email request using 'New System Request form' to the IT department and Head of IT and get the special policy allow approved by Head of IT.
2. All domain creations request comes through HR & respective Managers using 'New System Request form' to the IT department and Head of IT.
3. Head of IT shall be the formal authority for approving all domain connections and special as "Exceptional" connection.

L. Log Management

1. The user authentication logs from the OS and other function specific applications, web portals etc. should be monitored on a continuous basis.

2. The important threat indicators should be tracked during the periodic review of the logs. The indicators are listed below, but are not limited to:
   - Greater than three (3) failed login attempts for a user ID.
   - Attempts to access super user accounts.
   - Attempts to modify user privileges etc.

M. Hardening Guidelines

1. BIOS should be password protected, with password available to only the Network Security team.

Patch Level

The operating system should have requisite patches installed, having at a minimum,

- Windows 2008, Service Pack 1
- Windows 2012 Server
- Windows 7 with latest Service Pack if any
- Windows 8 with latest Service Pack if any
- Windows 10

2. The WSUS services should be configured to receive further updates from corporate patch management server of DMCC Local Security Policy

Account Policy

- Enforce Password History: 3
- Maximum Password Age: 60 days
- Minimum Password Age: 55 days
- Minimum Password Length: 8 characters
- Password must meet complexity requirements: Enabled
- Account Lockout Duration: 10 minutes
- Account Lockout Threshold: 5 attempts
- Reset Account Lockout Counter after: 10 minutes

Audit Policy

- Audit Account Logon Events: Success & Failure
- Audit Account Management: Success & Failure
- Audit Logon Events: Success & Failure
- Audit Object Access: Failure
- Audit Policy Change: Success
- Audit Privilege Use: Failure

1. **Security Options**
   - Network Access: Allow anonymous SID/Name translation: Disabled
   - Network Access: Do not allow anonymous enumeration of SAM accounts:
   - Enabled Network Access: Do not allow anonymous enumeration of SAM accounts & shares: Enabled
   - Accounts: Administrator account status: Enabled

- Accounts: Guest account status: Disabled
- Accounts: Limit local account use of blank passwords to console login only: Enabled
- Accounts: Rename administrative account: Rename as “sysoa“
- Audit: Shutdown system immediately if unable to log security alerts: Enabled
- Devices: Prevent users from installing printer drivers: Enabled
- Interactive Logon: Do not display last user logon name: Enabled

Information Security Continuity Policy

Introduction

- DMCC recognizes the criticality and need of its business and understands the importance of the availability of its managed services.
- The Information Security Continuity Policy defines the controls to establish a framework to counteract interruptions to business activities and to protect the critical business processes from the effects of business disruptions such as major failures, disasters, etc. and their timely resumption.

Purpose

- This document (The Information Security Continuity Policy) highlights a contingency action plan to ensure continuation/ restoration of activity in the event of an unexpected crisis, which could affect the normal functioning of the activities carried out by
- This Information Security Continuity plan covers the following:
  - Key services
  - Key resources of the organization
  - Key Assets
  - Business Impact Analysis and Risk Assessment
  - Containment Plan

Objective

- DMCC Information Security Continuity Policy is designed to meet the following objectives in the event of any disasters and calamities.
- Ensure safety of its employees.
- Protect and ensure the availability of all Information and Information processing assets.
- Maintain operations and continued support to all clients.
- In spite of best precautions, if a disaster does occur, causing interruption of services, the plans have provisions to meet the following objectives:
- Affect a sustainable recovery of operations that have been interrupted within the best possible time and provide the required support to applicants and
- Reduce the damages caused by any interruption in its business.

Scope

- All information assets of the DMCC are under the scope of this document

Policy Statement

A. *Key services*

1. IT Infrastructure
2. Applications

B. *Key resources*

1. Staff - Provision of services is dependent on the knowledge and skills of existing staff.
2. Premises – The Head office of DMCC is located at Prospect Chambers, Fort Mumbai. The main Data center is hosted at HO and plant office has a local Server room at premises.

3. Information Technology - The data, software, hardware - file servers, PCs, printers etc., structured cabling for data and telephony, LAN equipment and WAN equipment.

C. *Key Assets*

1. The Assets which are classified as Enterprise critical and Mission critical in Asset Register are considered as a key asset for the organization.

D. *Business Impact Analysis and Assessment*

1. When any of the disasters listed occur, they are likely to cause some disruption of the business. This disruption can impact business in many ways.
2. Sometimes the impact can result in service unavailability, loss of lives, regulatory non-compliances, customer dissatisfaction, penalties, financial loss, etc.
3. Hence it is necessary to analyze the impact of the disruption to assess the severity of impact in order to design appropriate recovery procedures.
4. It is envisioned that business interruptions could potentially occur on account of disaster events in the following key areas:
   - Natural calamity
   - Man-made calamity
   - Technology failure
   - Environment calamity
   - People failure

E. *Containment Plan*

1. This section details the steps to be taken if the business continuity is threatened by any event listed in the preceding pages. The containment strategy identifies actions to be taken prior to, during and following a business interruption to safeguard human life and conserve the assets, which can be salvaged.

a. <u>Natural calamities</u>

- Although natural calamities such as earthquake and floods cannot be contained, the building has facilities like emergency exits to ensure brisk evacuation of employees and applicants.
- From a fire perspective, the building has appropriate emergency exits.
  - i. On sounding of the fire alarm, the following activities to be performed:
    - Ascertain the location of the fire or emergency
    - Ensure that the alarm is audible
    - Ensure that all persons on the floor have been notified
    - Assemble all occupants in the assembly points or communication point
    - Establish communications with the emergency command station post in the vicinity of the assembly or communication point
    - Ensure that the evacuation is via an uncontaminated stairway
    - All persons are accounted for and injured given first aid.
    - Ensure lifts are not used during evacuation.
  - ii. Evacuation of the Premises shall be carried out as per evacuation plan set by ERT (Emergency Response Team).

iii. Employees and Applicants shall, gather in the designated fire assembly area. They shall disperse only after head count and further instructions.

b. <u>Man-made calamities</u>

- Although man-made calamities such as bomb threats, terrorist attacks, cyber-attacks and civil unrest cannot be contained, the building has facilities like emergency exists to ensure brisk evacuation of employees.
- From a bomb threat perspective, the building has appropriate emergency exits. The following activities to be performed:

i. Ensure that all persons on the floor have been notified

ii. Assemble all occupants in the assembly points or communication point

iii. Establish communications with the emergency command station post in the vicinity of the assembly or communication point

iv. Ensure that the evacuation is via an uncontaminated stairway

v. All persons are accounted for and injured given first aid.

vi. Ensure lifts are not used during evacuation.

c. <u>Technology failures</u>

- **Application/Tool Failures**

i. Team Lead in Application support team shall do the vendor coordination for application bugs Application Functionality Limitations / Issues (reported by partners), New Application Upgrades.

ii. Application team will also coordinate with the Authority and shall raise emails for the issue.

- **Hardware Failure**

i. DMCC has trained team for the server management and for major issues vendor support is available.

ii. DMCC has outsourced the hardware maintenance services with various hardware service providers.

iii. Hardware support team is also available onsite for troubleshooting any hardware issues.

- **WAN Failure**

i. DMCC has skilled and trained network administration personnel who shall monitor the WAN on a regular basis. Redundant ISP link is available for different geographical locations.

ii. SLA agreements with multiple service providers are available.

iii. There is support from external vendors who are skilled in managing such network components.

- **Power failure**

i. In the event of failure in regular power supply from service provider, the business operations can be continued through available UPS of adequate capacity.

ii. This UPS system has been installed and connected with all information systems and is extended to desktops. Diesel Generators are also available.

F. BCP Organization – Roles and Responsibilities

1. Every individual plays a critical role in the recovery process to facilitate the complete plans and processes. Business Continuity Manager and ERT shall work in collaboration and sync to each other for every aspect of recovery.

a. <u>ERT Team</u>

- Emergency Response Team should follow the procedure as follows once the disaster happens:
  i. ERT shall declare and communicate to the Business Continuity Manager that a disaster has struck
  ii. Action plan for emergency stages and scenarios.

b. <u>Business Continuity Manager</u>

- Business Continuity Manager shall be the operational body for business continuity operations and he shall facilitate the complete process of business continuity in the event of a major disaster.
- The Business Continuity Manager shall assess the damage provide details to Emergency Response Team.
- Business Continuity Manager shall maintain the contact details of key personnel from the emergency response team.
- Business Continuity Manager shall lead in evacuation of the employees through the safe path (like the emergency door).
- Procedure for raising alarms, communication with outside agencies, including emergency services shall take care by Business Continuity Manager.

G. *Business Continuity and Disaster Recovery Process*

1. The Business Continuity Plan lists down all various phases and procedures that need to be taken care of while adopting any recovery strategy for restoration of services.

a. <u>Notification and activation phase</u>

- The notification phase defines the initial actions taken once any disaster happens and one or many critical resources are not available for an extended period.
- In an emergency, the Business Continuity Manager’s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation Phase.
- Any employee and applicant encountering a situation that threatens life or property may decide to implement personal safety responses appropriately and immediately.
- Life must be protected before property in all instances.
- This phase includes activities to notify recovery personnel, assess damage to ongoing projects and business, and work on the BCP plan.
- Business Continuity Manager has been assigned for Call Tree notification.

b. <u>Notification Procedure</u>

- An emergency event may occur with or without prior warning. The notification process shall be the same in either case.
- The manner in which personnel are notified depends on the type of emergency; and whether the emergency occurs during or after normal business hours.
- Notification during normal business hours shall be accomplished by phone, e-mail, word of mouth, cell phone or by activating the Team Call Tree.
- Notification after normal business hours shall be conducted by activating the Team Call Tree.

c. Damage Assessment Process

- The Business Continuity Manager shall perform damage assessment based on the information provided by responder.
- After the assessment conducted by Business Continuity Manager, shall notify the ERT Team. Based on the available information the ERT Team shall determine the level of the emergency event.
- There are three emergency levels: Level 1, 2 or 3, which are explain in below table.

Level	Incident Category	Impact	RTO	RPO
Level 1	Environmental/system related (e.g., power failure, equipment failure)	Service is unaffected	1 day	5 mins
Level 2	Human (e.g., bomb threat, biological or chemical threat)	Service is affected	1 day	5 mins

d. Recovery Phase

- Recovery operations begin after the BCP is activated, damage assessment(s) is completed, ERT Leads and other team leads are notified, and recovery and services continuity are activated.
- The recovery phase focuses on contingency measures to activate temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new site.
- BCP team agrees the resource requirement with the disaster recovery team.
- At the completion of the Recovery Phase, normal recovery process shall be invoked.

e. Recovery Strategy

- This portion of the plan deals with actions to be taken to minimize the time taken to restore business after a business interruption and build a coherent plan for restoration of Business as Usual [‘BAU’] activities.

f. Recovery Point Objective

- Recovery Point Objective (RPO) is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

g. Recovery Time Objective

- Recovery time Objective (RTO) is the timeframe within which recovery must occur to an acceptable level as defined by management.
- In case of an eventuality, the first step would be to assess the extent of damage caused to any, or all of the above.
- Based on the assessment report of the damage caused, the ERT shall decide on whether operations can continue at the same premises, after taking into account the cause of the damage, extent of damage, recovery time required to get back to normalcy etc.
- If after assessment of the damage, it is decided that the same premises can be operational, the next steps would be to parallel work on making alternate arrangements for continuity of operations, apart from rectification of the impacted area.

h. Recovery Planning

- A key activity in planning for disaster recovery is to identify key system components and predict the types of failures that may occur.

- Business Continuity Manager in coordination with Emergency Response Team performs the following functions:
  - i. **Phase 1:** Alternate Processing Site Coordination Recovery – The coordination of the restoration of all critical IT services at the alternate site.
  - ii. **Phase 2:** Network Recovery – The planning and execution of recovery efforts related to data and video communications.
  - iii. **Phase 3:** System Restoration – The coordination of the restoration of all infrastructures-based computer services, voice, and data communications. Recovery is accomplished by having Managerial, Response, and support teams acting upon the contingency event that activates the BCP.

i. <u>Reconstitution phase</u>

- Based on the kind of disaster, it may be possible to restart the services from the affected site after some time.
- Once the recovery has been made at the primary site and operations are stabilized, the team at the affected site should work on recovering the site.
- Once this recovery has been made, the switchover back to the primary site needs to be done carefully after planning and informing to the Authority.

H. *Information Systems and Communications*

Paper Records

- Some important information may exist solely in paper form; this includes but not limiting to:
  - i. System documentations
  - ii. Operational Manuals
  - iii. Agreements
- Copies of such documents are scanned and stored in file server securely for future reference. Paper documents are kept in fire safe vault.

Policy for Data Privacy and Disclosure of Information

Introduction

- DMCC is committed to handling Personal Data responsibly in order to earn and preserve the trust of DMCC Employee and any third party interacting with an entity of DMCC.
- This Policy defines the main principles applicable to the Processing of Personal Data by DMCC India with a view to guarantee every individual's right to privacy. This Policy defines high-level standards as a minimum requirement in order to ensure an adequate level of protection within DMCC for the collection, use, disclosure, transfer, storage and other Processing of Personal Data.
- The policy document is formulated by assessing the existing processes at DMCC while referring the Data privacy guidelines and requirements stated in ***Indian IT Act Rule 2011*****.**
- "Sensitive personal data" means personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or which concern health or sex life, password, biometric, financial information such as Bank account or credit card or debit card or other payment instrument details This excludes any information that is freely available or accessible in public domain or furnished under the RTI or any other similar law.
- "Biometric" means technologies that measure and analyze human body, characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

Scope

- This Policy applies to DMCC and to all DMCC Employee Processing Personal Data
- All information assets of the DMCC are under the scope of this document

Policy Statement

A. *PERSONAL DATA PROCESSING*

- DMCC Employee and third parties Processing of Personal Data on behalf of DMCC must comply with the following Processing principles.

1. Consent should be in writing through letter or fax or email or in digital form from the Data subject regarding purpose of usage before collection of such information.
2. Only collect, use, disclose or store Personal Data for a specific, legitimate and necessary purpose.
3. One shall not collect sensitive personal data or information unless —
   i. the information is collected for a lawful purpose connected with a function or activity of the DMCC or any person on its behalf; and
   ii. the collection of the sensitive personal data or information is considered necessary for that purpose.
4. Ensure that the Data subjects are informed of the processing, fact that the information is being collected, intended recipients, agency for collecting & retaining information.
5. Disclosure of sensitive personal data or information by DMCC to any third party shall require prior permission from the Data subject, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between DMCC and Data Subject, or where the disclosure is necessary for compliance of a legal obligation or by an order under the law for the time being in force.
6. Only retain Personal Data for as long as is necessary for the purpose for which they are processed, in compliance with local legislation.

B. *SECURITY AND CONFIDENTIALITY*

1. Protect these Personal Data while they are being collected, processed, used, disclosed, stored, and transferred internationally.
2. Ensure the security of processed personal data.

C. DATA SUBJECTS' RIGHTS

1. Data subject must be permitted, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.
2. Prior to the collection of information including sensitive personal data or information, provide an option to the Data subject to not to provide the data or information sought to be collected.
3. The Data subject shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to DMCC. Such withdrawal of the consent shall be sent in writing to DMCC. In the case of Data subject not providing or later on withdrawing his consent, DMCC shall have the option not to provide goods or services for which the said information was sought.

D. SENSITIVE PERSONAL DATA TRANSFERS

1. Domestic/International Transfer of data is allowed only if it is necessary for the performance of the lawful contract between Sanofi or any person on its behalf and Data subject or where such person has consented to data transfer.
2. The Transfer should only concern Personal Data which are relevant and not excessive for the purpose of the Transfer.

E. RESPONSIBILITIES

1. The Grievance Officer shall redress any discrepancies and grievances of the provider of the information with respect to processing of information.
2. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.
3. If in doubt, consult your superior or the Grievance officer PrivacyGrievanceOffice@DMCC.com

Key Definitions

Term	Definition
Employees	Refers to DMCC (Full time, part time, temporary, etc.) and contract employees
Information systems	DMCC's information systems include, but is not limited to, operating systems, applications, databases, computing systems, networks and networking devices.
Head of IT	The employee who is the head of the Information Technology & systems department.
Department/ Functional HOD	The employee who has been designated as the head of a department or a function.
Systems in-charge	Employee who holds key responsibility for implementation, administration and support of respective IT services and applications.
Technical team	The team in the IT department responsible for implementation, administration and support for data center and critical IT services.
Network Security Team	The team in the IT department responsible for responsible for installation, configuration, monitoring and maintenance of all network

Term	Definition
	components along with handling access granting procedures for business specific servers.
Operations Team	The team in the IT department responsible for deployment, support, service, maintenance and disposal of end computing assets and peripherals.
Application team	The members of the IT team who are responsible for supporting the deployed applications.
Access controls	The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises.
Access rights	The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information technology policy.
Confidential information	Confidential information includes, but is not limited to, client list, employees' performance reviews, salary details, trade secrets, passwords and information that may affect DMCC and its employees, if the information were disclosed to the public.
Shared accounts	Shared account is a generic user ID assigned for one specific role that can be used by more than one person.
Network components	Network components include, but is not restricted to, all the components that are present in DMCC's IT infrastructure namely switches, routers, servers, firewalls, access points etc.
Internet Service Provider (ISP)	This is an organization that provides services for accessing, using, or participating in the internet.
Advanced Encryption Standard (AES)	This is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).
Antivirus Software	This is a computer software used to prevent, detect and remove malicious software.
Cipher Block Chaining Message Authentication Code Protocol (CCMP)	This is an encryption protocol designed for Wireless LAN products.
Data loss prevention (DLP)	Data Loss Prevention Products help a network administrator control what data end users can transfer, thereby ensuring that sensitive data does not leave the corporate network.
De-Militarized Zone (DMZ)	This is a physical or logical sub network that contains PPFL's external-facing servers/services to the internet.
Encryption	It is the process of encoding messages or information in such a way that only authorized parties can read it.

Term	Definition
External media	External media includes, but is not restricted to, portable storage devices like compact disks, USB storage devices, portable hard disks etc.
Firewall Rule base	This is a set of rules that govern what is and what is not allowed through the firewall.
Hyper Text Transfer Protocol (HTTP)	This is an application protocol for distributed, collaborative, hypermedia information systems.
Internet Assigned Numbers Authority (IANA)	A non-profit private American corporation that oversees global IP address allocation.
Intranet portal	An intranet portal is the gateway that unifies access to enterprise information and applications on an intranet and a part of it published in internet.
IP addressing	The procedure that involves, but is not limited to, assigning and managing IP addresses to all assets present in PPFL's IT infrastructure.
Network components	Network components include, but is not restricted to, all the components that are present in PPFL's IT infrastructure namely switches, routers, servers, firewalls, access points etc.
Network Time Protocol (NTP)	This is a networking protocol used for clock synchronization across all IT assets at PPFL's corporate head office, to ensure that the timestamp on the logs at any instant remains the same.
Network zones	These are logical LAN segments set aside for a specific function or IP Range
Networking devices	Network devices are components used to connect computers or other electronic devices together so that it can share files/resources like printers or fax machines.
Other external support users	Personnel other than employees who are deployed for PPFL directly or indirectly and need access to PPFL information assets/IT services for performing their activities.
Server Farm	Also known as a server cluster, it is a group of networked servers that are housed in one location.
Service Set Identifier (SSID)	This is a sequence of characters that uniquely names a wireless local area network (WLAN).
Transmission Control Protocol (TCP)	This is a standard that defines how to establish and maintain a network communication channel via which application programs can exchange data.
Two-tiered network architecture	This refers to client/server architectures in which the user interface runs on the client and the database is stored on the server.

Term	Definition
Unified Threat Management (UTM)	Also called Smart Firewall. These are security appliances that provide administrators the ease of handling multiple functions like antivirus, content filtering, intrusion prevention and spam filtering functions under one roof.
Universal Serial Bus (USB)	This is an industry standard developed to standardize the connection of computer peripherals.
Virtual Local Area Network (VLAN)	They have the same attributes as a physical LAN but allow Administrators to logically group workstations even if they are not located physically on the same LAN segment.
Data Subject	An identified or identifiable natural person to whom the Personal Data that are being Processed relate; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.
Personal Data	Any information relating to a Data Subject;
Sensitive Personal Data	Personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or which concern health or sex life, password, biometric, heath record, financial information such as Bank account or credit card or debit card or other payment instrument details This excludes any information that is freely available or accessible in public domain or furnished under the RTI or any other similar law.
Biometric	Technologies that measure and analyze human body, characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;
Consent	Data Subject’s freely given specific and informed indication of his/her wishes by which the Data Subject signifies his/her agreement to the Processing of his/her Personal Data for the purposes described.
Personal Data Processing	Any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
Personal Data Transfer	Any Data disclosure, copy or move via a network (e.g. remote access to a database) or from a medium to another regardless of the type of medium;
Recipient	Natural or legal person, whether a Sanofi entity or a third party, to whom/which Personal Data are disclosed;

Version Control and Approvals

Process Owner					
Change/Revision History					
Sl. No.	**Version**	**Change Incorporated**	**Prepared By (Signature and Date)**	**Reviewed By (Signature and Date)**	**Approved By (Signature and Date)**
1.	1.0				