KANINI
Excellence Redefined

Table of Contents

KANINI
Excellence Redefined

Office Decorum

Applicable to	*All employees*
Responsibility	*Human Resource Department and Chief Operating Officer*
Periodic review of policy	*Human Resource Department and Chief Operating Officer*
Purpose	*To ensure that the adequate information is provided to all employees about the office decorum to be adhered within the organization*

1.1 Office Timing

All employees are expected to be regular and punctual in attendance. Employees should reach the office well in time to actually start work at the designated start times.
General Shift: 11am – 8pm, Exceptional based on the project team

1.2 Policy on Leave

A. Objective

This policy provides a format system

- to avail leave during active service with the company and account for absence from work for personal reasons
- to grant leave for the employees to meet exigencies

B. Applicability

This policy is applicable to all full-time employees, serving probation and trainees of the organization from the date of their joining the regular service.

C. Eligibility

Limits and applicability are as per guidelines given below.

D. Types of leave

a) **Earned leave**: Below mentioned plus 9 Government(State & national) holidays

Years of Exp	No. of CL
0-2yrs	12 days
2.1-5yrs	15 days
5.1-8yrs	18 days
8.1-10yrs	21 days
10+ yrs	24 days

b) Privileged leave: Additional leave benefits to accommodate various other leaves.

c) Sick Leave: Employees can make use of these leave types when they are not well.

d) Compensatory off: This can be claimed when employees work additional hours for project needs and billed at client end.

e) Wedding leave: 1 week

- Wedding leave can be availed only after the completion of 6 months with Kanini.

f) Maternity leave: Apart from the below, we always adhere government regulations whenever it is amended.

- According to the above Act, a woman is entitled for maternity leave, once she completes her 80 days with the company.
- Pregnant women are eligible for 6-months(3 months fully paid + 3 months with basic salary) maternity benefits.
- Female employees can avail 4-6 weeks of WFH / unpaid leave post the 6 months maternity benefits
- Employee can choose to take after delivery or before delivery

E. **Notice Period –** All employees to serve a notice period of 90 days from the date of resignation. Also, all the leave balances and benefits will be frozen during this period. Any leave availed during this period, it will invite LOP and/or extension of the notice period as per the criticality and dependency of the project.

F. Leave Encashment

- ≤ 6 days leave will be carried over to Next year.
- Balance leave post above calculation from the above will be enchased calculating the basic pay of the employee.
- Leave encashment is applicable only for **Earned leaves & Compensatory offs**

G. Operating guidelines

- Leave year is from 1st January to 31st December of a calendar year.
- For employees, who joined in the middle of the year, eligibility is calculated on a monthly basis.
- Absence from work more than 3 days continuously without intimation will lead to termination of the position. No response to “Showcause letter” also will lead to termination.

- Intervening weekly off/ holidays will not be counted as leave but in case of long leaves/ wedding leaves, the intervening holidays will not be paid for.
- Absence from work needs to have the approval of appropriate authority before proceeding on leave.
- Where the employees are not able to inform in prior, it is required that the individual should inform her/ his immediate lead.
- For new joiners (probation period) – Accumulated leaves can be taken but following month's leave cannot be availed previously.
- Leave encashment will be calculated on the basic pay as of previous year 31st Dec.
- An employee working on weekends should avail comp-off in the following two weeks itself else it will lapse.
- Earned leave will not be compensated for notice period.

H. Trainees

- One leave per month can be availed during the training period.

I. Late In/ Early out with Prior Permission

Employees can avail monthly two permissions ie. Two hours each. Exceeding two hours would be considered as half day leave/month.

1.3 Dress Code

All employees are expected to be properly groomed and wear proper formal dress.

- Mon-Thur – Formal wear / KANINI T-shirts
- Friday – Casuals (No shots(3/4ths), No torn jeans, No skirts, No sleeveless) + KANINI T-shirts

1.4 Cleanliness

Employees are expected to keep their surroundings neat, clean, and tidy. Use provided dustbins to dispose of any wastes. Each employee must take responsibility for the workplace, dining hall, and of the office in general.

1.5 Work from home policy

A. Policy Statement

Work at home was brought in for the situation where employee has to complete the task on the same day but he/she cannot be present in the office for unavoidable situations.

The employer recognises that there may, on occasion, be circumstances when it would be more beneficial or flexible for staff to work at home. However, it is not possible to offer home working to all staff as the requirements of some jobs will not be suitable for such arrangements.

B. Qualifying conditions

- Prior permission is required before an employee can work at home.
- Unavoidable situations may arise where an employee cannot get prior approval, In that case he/she has to talk to the immediate lead and explain the situation. Immediate lead will take a decision for work at home based on the criticality.
- Immediate lead has to drop mail to other leads stating that the concern employee will be working from home for the specific reason.
- After the permission is granted, Employee has to send in the mail listing the tasks he is going to work on and same has to be sent at the end of the day stating what has been completed and what not.

C. Working arrangements

- Proper VPN connection has be taken for certain projects.
- No other tools like Team viewer / Ammy can be used.
-

1.6 ID Card / Access Card

Employees are required to wear ID cards prominently displayed all times while inside the premises at work. Entry inside the premises will not be allowed without an ID card.

Access card needs to be submitted to the security while leaving the premises everyday for probation employees.

1.7 Unauthorized Access

Employees are not allowed to use company infrastructure to download or install any personal, illegal, or unauthorized program, software, or data.

KANINI
Excellence Redefined

Disaster Recovery Policy

Applicable to	*All employees*
Responsibility	*Human Resource Department and Chief Operating Officer*
Periodic review of policy	*Human Resource Department and Chief Operating Officer*
Purpose	*To ensure that the adequate information is provided to all employees about the office decorum to be adhered within the organization*

2.1 Objective

- A disaster is a serious incident that cannot be managed or pre planned. We can only frame few procedures that should be followed at that time.
- This policy provides a framework for the ongoing process of planning, developing and implementing disaster recovery management for all-natural calamities faced by Kanini.
- This policy is implemented to minimize the impact of significant incidents at Kanini through a combination of responsive and recovery controls.

2.2 Disaster Recovery Management

- Disaster Recovery Management consists of 4 team members.
- At the point of any disaster, security has to contact one of the DRM. DRM contact details will be readily available with the security as soon as they join.
- Disaster Recovery Plan (DRP), which contains all instructions to be followed for most of the natural calamities, is with DRM and security.

2.3 Expected Natural Calamities

1) **Cyclone disaster**
    - Instructions to be followed in DRP
2) **Fire disaster**
    - Instructions to be followed in DRP
3) **Flood disaster**
    - Instructions to be followed in DRP
4) **Earthquake**
    - Instructions to be followed in DRP

KANINI
Excellence Redefined

Clean Desk & Clear Screen Policy

Applicable to	*All employees of Kanini*
Responsibility	*Head of Operations*
Periodic review of policy	*Information Security Officer & Information Security Forum*
Purpose	*To set access controls at an appropriate level on need to use basis which minimizes information security risks yet allows the business activities to be carried without undue hindrance*

3.1 Clear Desk

All employees will adopt clear desk policy for papers and removable storage media in order to reduce the risks of unauthorized access, loss of, and damage to information while leaving their workstations for a long break or at the end of workday. The following controls are considered for the same:

- Work material should be secured in a locked area while not in use.
- Any work material that is discarded is shredded and any information contained therein cannot be retrieved.
- Sensitive or classified information, when printed will be cleared from printers immediately.
- Confidential documents will not be left on workstations unattended.
- Managers should, in addition, lock their rooms while stepping out of office.
- Security shall have keys to all locked rooms and all locked areas to handle emergencies. These extra keys should be kept in locked custody in entrance lobby and not easily accessible to an intruder.
- Surprise sweeps of desks shall be conducted at least once a quarter to ensure the clean desk policy is fully complied with.

3.2 Clear Screen

All employees will adopt clear screen policy for their desktops, laptops and servers in order to reduce the risks of unauthorized access, snooping, loss of, and damage to information during and outside normal working hours. The following controls are considered for the same:

- Systems should be locked while stepping out of workstation (‘Ctrl + Alt + Del’) or (Windows+L).
- All workstation desktop computers, servers, computer terminals and Laptop computers should be programmed to let a password protected screensaver to kick in when the

equipment has not been in use for more than a stipulated period to prevent unauthorized "snooping."

- Screen Timeout and Lockout – 2 minutes
- Technology services should ensure this is enforced and should review compliance at least once Quarter.
- All the Desktop Users will have organization provided screen savers.

Open Door Policy

An **open-door policy** is a communication policy in which a manager, COO, MD, president or supervisor leaves their office door "open" in order to encourage openness and transparency with the employees of that company. As the term implies, employees are encouraged to stop by whenever they feel the need to meet and ask questions, discuss suggestions, and address problems or concerns with management. An open-door policy serves to foster an environment of collaboration, high performance, and mutual respect between upper management and employees.

Confidentiality and security policy

Applicable to	*All employees of Kanini*
Responsibility	*Head of Operations*
Periodic review of policy	*Information Security Officer & Human Resource Department*
Purpose	*To set access controls at an appropriate level on need to use basis which minimizes information security risks yet allows the business activities to be carried without undue hindrance*

5.1 Company and personnel Information

A. Data Protection: Employees & Contractors

Every employee or contractor for providing personal service (with necessity to access our premises or our data/information and files) shall be subject to a formal legally enforceable Non-Disclosure Agreement for employment or service provider in a format approved by an Head of Information Technology/Information Security Officer that includes following covenants in a reasonable/adequate form:

- No solicit of business from our customers
- No solicit of employees
- No circumvention to do business directly with our customers
- No disclosure of confidential information
- No infringement of intellectual property rights

No employee or contractor should be provided with temporary or permanent access cards to enter our premises unless and until a formal contract is signed.

B. Data protection: Vendors & Consultants

Technology services should ensure that every vendor/consultant who is in a position to access data or hardware containing data in the course of his work has entered into a Non-Disclosure Agreement with Kanini to not solicit business, not circumvent Kanini and reach customers and not disclose any such data to any third party.

Technology services should ensure that any vendor/consultant working on technology infrastructure is fully supervised by a full-time employee; and any asset leaving Kanini premises is backed up and blanked to minimize the probability of data loss/theft.

5.2 Mobile and landline usage

- Employees, Security guards and housekeeping staff's mobiles should be on silent mode as they enter the office premises.
- Office landlines should be used only for official purpose.

5.3 Access card activation & deactivation

- All employees, security guards, and housekeeping staff are provided with an Access Card to access the Work Facility.
- Every Access card contains a 4-digit number. For employees, that 4 digits is their last 4 numbers of employee codes.
- An employee's card access is deactivated when the employee leaves the organization by using Card Access Control System.
- The employee surrenders the Access Card to the HR during the exit formalities. The employee code is immediately deleted from the database.
- HR confirms the deactivated card by showing it to the card reader and ensures that an alarm is raised, and the door does not open.
- An absconded employee's Access Card is deactivated immediately after getting confirmation from his/her supervisor.

5.4 IT and Network Security procedures

A. Internet and E-mail access control

- YouTube and other social media websites are restricted to avoid productivity loss of the employees. Please raise a request to the CISO & respective managers if you need access to social media for learning.
- We have a separate network for guests(clients / vendors). Password will be shared upon request from concern team / HR
- All data transmitted through email / internet is the property of Kanini and bounded with laws in case of any unauthorized copying or misuse. The email facility shall be used in a lawful, professional and ethical manner.
- Employees shall communicate with their Managers during their long leave or vacation and handover the password for any immediate action on emails. Through outlook the employee can set the auto reply message with appropriate contact information / details.
- Any information that is marked as proprietary, confidential shall not be sent outside company through email or by any means. Unauthorized dissemination intentional or unintentional of such material shall result in severe disciplinary action with penalties or both.
- The password shall not be shared within groups or out of groups for any purpose.
- Disclaimer Statement is added for each email.

B. Laptop usage

Users are responsible for the safety, security, and upkeep of the same. Users must return laptops in as received condition whenever required to do so. Full disk encryption and necessary password protection is enabled.

C. Virus checking

Kanini desktops, laptops, and servers are protected with Mcafee. Mcafee is centrally administered by SQL Database and users cannot disable or tamper with Antivirus/Antispyware protection. If users obtain virus alerts, they must

call IT persons immediately for technical assistance. Users must not remove viruses on their own.

D. Testing/ Trouble shooting prohibition

Users must not test or attempt to compromise any information security mechanism. Users must report any technical issues like security alerts, errors, and warnings, etc., including keyboard/mouse issues to IT immediately. They should not do any troubleshooting to fix the issue.

E. User backup

Users must not store any data in local systems.

F. Server backup

- It is the policy of Kanini to ensure that timely back up is taken for the data in the server and the terminals are connected. Back frequency is defined for the Server and Terminals and is arrived by CISO
- The backup of server is taken on a daily/weekly basis. The backup will be taken on one of the hard drive of the server and stored (Internally).
- Parallel a copy of the backup will be taken in a external device called - NAS and this copy is placed at the CEO's residence to recover the data in case of emergency (externally).
- The backup details will be recorded in the Back up register by IT Admin team.
- Restoration of specific files from the backed-up data will be retrieved once a month by the IT Admin team to check the data as part of restoration process and same is evident in the back up register

G. Printer access control

- Printer accesses is maintained and controlled by IT.
- Production users are restricted printing access.
- Team Leads, Log/MIS, Managers, and Other Support users have access to printer's subject to business requirement.
- Unwanted papers need to be shredded in shredder which is provided at HR cabin.

H. Password Policy

- **Password Creation** - Password creation shall be documented, and the request shall flow from the Operations head to the CISO for approval and the same to be recorded. The passwords are transmitted orally to the user after creation, the same needs to be changed in next logon.

- **Password Inactiveness** – To resume password or revoke password, the request shall flow from the user through Operations Head with the reason and to be approved by CISO.

- **Password policy and Inactiveness** –

> The password shall have 3 combinations of below four

a. Capital case

b. Special character

c. Character

d. Number

> Logon attempts to lock – 3 attempts

> Inactive for the period, then disable – 7 days

> Password Lock

> System idle for 2 minutes, then resume with Password

> Enforce password history: 6 passwords remembered

> Maximum password age: 45 days

> Minimum password age: 1 day

> Minimum password length: 8 characters

> Password must meet complexity requirements: Enabled

> Store password using reversible encryption for all users in the domain: Disabled

KANINI
Excellence Redefined

I. Network security

Security: Firewall

Physical access to firewall should be controlled and restricted to a list of employees cleared by Head of Technology.

Security rules written into the firewall should:

a) Be simple,
b) Be void of redundant/old rules
c) Be consistent with security policy
d) Deny access to all traffic by default and enable specified services
e) Limit the number of applications running on firewall to facilitate maximum effectiveness (as far as possible antivirus, content filtering, VPN, DHCP and authentication should be run in dedicated devices behind firewall)
f) Not entirely dependent on packet filtering; should use state full inspection and application proxies wherever possible
g) Be run on a hardened and routinely patched operating system
h) Be used to segment internal networks logically to restrict applications
i) Be subjected to periodic analysis of vulnerability threats
j) Documented and signed off by CEO.

Security: Anti-Intrusion

Technology services shall install Intrusion Detection Systems and Intrusion Prevention Systems to deny access to malicious intervention into systems. The IP's chosen should provide real time analysis and prevention of attacks. The signatures in IDS/IP's should be current and valid. Event logs should be rotated, and a copy should always be written into storage.

Technology services shall ensure that all default user accounts and default user passwords are rendered unusable in all information-processing assets upon acquisition/installation of such an asset.

Technology services shall ensure that all data stored in central data storage and all transmissions are "encrypted".

Anti-Virus or Prevention of Malicious Code

Kanini shall formally prohibit the use, on any information processing system or device it owns or operates any software whose procurement was not carried out through Kanini purchase procedure.

Technology services should implement an "Anti-virus policy" that includes:

a) Protecting the network and all information-processing assets with current and valid anti-virus packages
b) Blocking malicious attachments coming with emails etc.
c) Automated updating of virus signatures on a continuing basis
d) Educating users on steps to be taken to avoid malicious codes

All operating and application software in all information-processing assets should be kept up to date by Technology services to ensure protection against latest threats added to software/application by manufacturer is available.

Software and any other files or folders shall not be transferred or downloaded onto Kanini Tech network via or from external networks, or on any medium including CD-ROMs, USB sticks, including during maintenance and emergency procedures, unless specific controls have been implemented.

Monitoring, detecting and deleting unauthorized software shall be carried out by Technology services as a requirement of information system.

Technology services shall act to identify and patch software and system vulnerabilities through Windows server update services in order to reduce the risk of malware attacks on all Kanini information systems.

Business continuity plans shall be implemented to make specific provision for recovering from malware attacks.

Physical Security Controls

Applicable to	*All employees*
Access to	*All employees*
Responsibility	*Chief Information Security Officer*
Periodic review of policy	*Chief Information Security Officer & Information Security Forum*
Purpose	*To ensure that the adequate information is provided to all employees about the information security practices to be adhered to within the organization*

6.1 Objective

This document describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or unrecognized attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, locks, access control protocols, and many other techniques.

6.2 Scope

All designated secure areas like Server room, Data Center, Disaster Recovery Site and any premises of Kanini, are subject to controlled access and usage.

6.3 Policy

- Main Entrance of the building is guarded by the security guard who is onsite for 24x7.
- Entrance of work facility is controlled by facial recognition system and is monitored by Security Guard.
- Authorized persons are only allowed inside the work facility.
- Every employee is assigned with an authorized card to access the work facility, if needed
- Every employee authorized to work in facility is issued with photographic identification card. This identification card is carried out by every employee during the work time and is displayed up front while working inside the facility.
- Failing to bring the access card and photo identification card has to report to the HR immediately and temporary card is given to employee by taking his/her signature.
- Card access is deactivated when an employee leaves the organization by using card access system and HRMS.
- Telephones inside the work facility are limited by technical control and only used for official purpose.
- Fire extinguishers are placed inside the work facility and we have formed an ERT (Emergency Response Team) to support and guide employees.
- Non-work-related visitors are not allowed to visit the employees inside the work facility.
- Visitor make entry in the visitor register and given a visitor pass, visitor passes do not provide access to any area in the premises. Visitor badges should be different and easily identifiable from employees.
- Work related visitors (such as vendors) are allowed inside the work facility after checking and are provided with visitors pass.
- Visitor passes must be returned to the security at the time of exit.

- Orientation on security control is given to the employee at the time of induction and is advised to report immediately to the management or guard against any security violation.
- Entry and Exit of housekeeping staff is monitored by access card system. They are allowed inside the work facility after supervision by the security guard. Photographic identification card is provided to the house keeping.

a) Server room

- Entry and Exit to server room is monitored by finger print access.
- Server room access is limited to COO & CFO, IT admin and HR for some emergency purpose.
- Externals coming in for service, maintenance are accompanied in server room with either HR or IT admin.

b) UPS room

- Entry and Exit to UPS room is maintained by the manual register.
- UPS room access is limited to COO, IT admin, HR and Security only.
- Externals coming in for service, maintenance are accompanied in UPS room with Security, IT admin or HR.

c) Conference and Training hall

- Conference and training hall is open to all Kanini employees with prior booking by notifying the facility manager.