ROSMERTA GROUP

IT POLICY & GUIDELINES

EFFECTIVE DATE

1st April 2024

POLICY No. & VERSION

IT / 01/ 2024 / Version 1.0

Contents

IT Policy - Acceptable Use Policy

Objective

The objective of this policy document is to outline the acceptable use of IT assets of RTL and its group companies. The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at RTL in conjunction with its established culture of ethical and lawful behaviour, openness, trust, and integrity. These rules are in place to protect the employees and company as inappropriate use exposes company and employees to various risks including loss of information, theft of assets, virus attacks, compromise of network systems and services, legal and reputational issues and to maintain the confidentiality, integrity, and availability of its information assets.

Scope

This policy applies to all employees of the company across all locations

Policy Guidelines

- Any digital devices that connects to the RTL 's network must comply with RTL 's IT Policy.
- Company provides various IT assets to various users to carry out their work related to business of RTL . While company desires to provide a reasonable level of privacy, users should be aware that the data/information they create/store on any system/hard copy remains the property of company.
- Though IT team will take all measures to protect the company network and systems, management cannot guarantee the confidentiality of individual / personal information stored by the employees on any digital device belonging to the Company.
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic as per the Audit Policy.
- Devices that interfere with other devices or users on the RTL network may be disconnected.
- The employee shall take due care and necessary approvals while disposing off/ destroying / shredding Confidential Information.
- Each user is responsible for exercising good judgment regarding appropriate use of RTL 's IT resources in accordance with RTL 's policies, standards, and guidelines.
- All PCs, laptops and other digital devices must have a feature to lock the screen or log off when the device is unattended for a maximum of 10 minutes.
- The employee shall promptly advise their immediate supervisor and IT team, if they discover that there is any security risk.
- Management reserves the right to disclose all communications, including and not limited

to text and voice, to law enforcement agencies or other third parties in compliance with legal, statutory and regulatory requirement

- Users shall collect their printouts immediately from the printer
- Discussion of Confidential Information over phone in public places should be avoided
- Following is expressly prohibited:
    - Causing a security breach to either RTL or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
    - Causing a disruption of service to either RTL or other network resources
    - Introduction of malicious programs into the network or server (e.g., viruses, worms, etc.) or introducing honey pots, honey nets, or similar technology on the RTL network.
    - Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted information, and software.
    - Use of the Internet or RTL 's network that violates the RTL 's Internet Policy, its network policies, or local laws.
    - Port scanning or security scanning on any RTL network unless authorized in advance by CTO.
    - In-appropriate use of communication means and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates RTL 's policies against harassment or the safeguarding of confidential or proprietary information.
    - Sending Spam via e-mail, text messages, pages, whatsapp messages, voice mail, or other forms of electronic communication.
    - Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
    - Use of a RTL 's e-mail or IP address to engage in conduct that violates RTL 's policies or guidelines.
    - Unauthorized copying of copyrighted material including, but not limited to, installation of any licensed software without formal approval from IT
    - Revealing one's account password to others or allowing use of your account by others.
    - Using a company provided computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or any other laws.
    - Making fraudulent offers of products, items, or services using any IT system of the company.
    - Blocking authorized audit scans
    - Providing information about, or lists of, RTL employees, to parties outside company is prohibited unless approved by the HOD or management.
    - Use of an e-mail account that is not provided by RTL or its customer and partners

for carrying out company's business.

- Storage of proprietary information on any personal device or sharing with non-RTL controlled environments, including devices maintained by a third party with whom RTL does not have a contractual agreement
- Downloading, installing or running security programs or utilities that reveal weaknesses in the security of a system.
- Registering using company's email id on public sites like Zomato, Swiggy, Amazon, Flipkart, Facebook, Twitter or any other site for personal use.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Password Policy

Objective

The objective of this policy is to ensure secure use of Company's IT assets (Hardware/Software) by setting up of rules for IT Team and Users for deployment of strong passwords and for changing them periodically to make sure that only authorized people can access those assets and data.

Scope

This Policy is applicable to all hardware and software assets in the organization viz.:

- End user equipment including Desktops, Laptops
- Network and Security Devices including Firewall, Wi-Fi, Switches, Network Printers, Other devices
- Applications – Both in house and bought including e-mail and others
- Data Centre Equipment (whether at own premises or hosted at 3rd party) – Servers , Storages, Other Equipment

Policy Guidelines

<u>Password Policy Guidelines for Users</u>

- Each user is responsible for safekeep of all his / her passwords
- All users must change their password on 1st login
- All users need to change their passwords every 90 days or earlier. This includes passwords for system login, email and various applications
- Minimum Password length has to be 10 Characters and must include at least 1 alphabet in upper case, 1 alphabet in lower case, 1 number and 1 special letter. (Upper and lower case characters are like a-z, A-Z; Special characters are like!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) while Numbers are like 0, 1, 2 to 9). Examples for password could be Ayhrdt@451, 1#NowQW45@, RdIKks@#628!
- While keeping password, please remember that you should not use following as part of your passwords
    - Names of family members, pets, friends, co-workers, fantasy characters, movies, TV serials etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses, city names and

phone numbers.
    - Word or number patterns like abcd1234, qwerty, 123456, 123321, Rosmerta 1, 1Rosmerta etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
    - Any passwords like admin, 1234, password, user, test, logmein, P@ssw0rd etc.)
- All passwords need to be treated as sensitive, Confidential Organizational information.
    - Do not share Organization passwords with anyone, including administrative assistants or secretaries.
    - Don't share any password in an email message
    - Don't reveal your password to your manager or other colleagues
    - Don't discuss about your password strategy / thought in front of others
    - Don't hint at the format of a password (e.g., "my family name")
    - Don't reveal any password on any questionnaires or forms
    - Don't share passwords with your family members
    - Don't reveal / share passwords with your co-workers while on going on leave / vacation
    - If someone asks you to share your password, please do not do that and contact IT department
    - Last 5 passwords should not be repeated
    - Do not use the "Remember Password" feature of applications or in browsers like Chrome, Edge etc.
    - Do not write passwords down or store them anywhere in your office.
    - Do not store passwords in a file on ANY computer system (including mobile devices) without encryption.
    - Do not keep same passwords for all applications
    - Do not use the same password for organization accounts (Rosmerta e-mail, Navision, HSRP, MIS and other systems) as for your personal access accounts like Gmail, Hotmail, Facebook, twitter etc, passwords in trading accounts, bank accounts or personal other accounts).
- If you believe your password may have been compromised, please change the password immediately and report the incident to IT Team

Password Guidelines for Database Administrators / IT Infrastructure and Application Team:

- Default login password for all equipment must be changed at the time of installation & configuration.
- All server, storage, Firewall, Wi-Fi, Network Switches, Application system accounts and other admin passwords should follow the same policy as for end users viz. Minimum Password length has to be 10 characters and password should contain at least 1 alphabet in upper case, 1 alphabet in lower case, 1 number and 1 special letter, passwords should

be changed every 90 days, Last 5 passwords cannot be repeated and all other guidelines as above.

- Some server administrator and Operating System / Database User account passwords may be exempted from being changed every 90 days due to application dependency on it (as application functionality is likely to be disturbed/stopped if there is any change in the administrator/admin password). Details of these exempted servers and application should be approved by CTO and should be reviewed by IT Infrastructure lead every 90 days.
- Every Desktop, Laptop must be configured with only following two Windows login accounts viz. Local administrator and User's account. Local administrator Password cannot be shared with anyone and all Operating System Guest accounts must be disabled.
- All system-level passwords (e.g. Administrator, root, enable, device administration logins, application administration accounts, etc.) must be changed when there is a change in role or employment of any system / database administrator.
- Passwords must not be shared in group mail; it should always be shared by one to one mail.
- Passwords for critical equipment's or applications must be shared between at least two members. List of such equipment and names of persons with whom password is shared should be approved by CTO.
- All the system level passwords should be written on a paper, put in a sealed envelope and should be kept in a fireproof cabinet or with CTO.
- All servers should have MFA (Multifactor authentication / two-factor authentication) using OTP etc.
- In case of any Application Manager requires administrator password and / or Remote access of the server for self or any vendor, they must provide approval from CTO mentioning the purpose and time period. Remote access of servers and other devices should be given only through VPN and all RDP/VPN login account provided to employees or External resources (Vendors) must be deactivated after the job is complete.
- When any Employee resigns from his / her job, all the user passwords (Email, any applications or system) must be changed by IT team on or before the last working day of the employee. HR department must ensure to share the list of such employee with IT department well in time.
- In Case of Resignation of IT infrastructure person, Application owner or Database Administrator, all administrator passwords should be changed and shared with the person who is taking handover

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - E-Mail Policy

Objective

The objective of this policy is to detail the usages guidelines for accessing company's email system. This policy aims to reduce the risk of email related security incidents and enable faster and better business communications and collaboration.

Scope

This policy applies to all employees of the company across all locations

Policy Guidelines

This policy is categorized in following three sections:

1. Email ID Activation Process
2. Email ID Deactivation Process
3. Email Usages Guidelines

Email ID Activation Process:

- This Email Policy is applicable to all Employees.
- Email ID must be allocated to all employees above the level of Assistant Manager at all locations. However, in case of corporate office, Email ID must be allocated to all employees
- For the employees below the level of Assistant Manager at locations other than corporate office, if e-mail ID is required then the request has to be approved by either Head of Department or HR. Similarly, if any existing employee who does not have an email id and needs to have an email id, he/she will get approval from HOD.
- In case of new joinees, HR Department will need to send approval for the activation of Email id for new joined employee along with the approval for IT assets that need to be given to new joinee.
- Following details are mandatory to be submitted by the requester to create an Email ID : Employee First name, Middle name, Last name or Surname, Employee Code, Department & Section, Location, Contact No.
- IT department will ensure to create the email id same day and share the details with the concerned person through phone call or personal meeting.
- Email id will be crated as Firstname.Lastname@rosmertatech.com or any other domain as determined by CTO. In case same name exist then id will be created as

Firstname.Lastname1@rosmertatech.com (or any other domain) or by adding / abbreviating relevant characters to fit the e-mail account creation criteria. The numeric value will increase if same first name and last name occurs and will be issued on first in first serve.

- Generic Email will be given only based on HOD or CTO Approval only.
- Email Access would be over the web (Browser – Google Chrome, Microsoft Edge) or mobile device only.

Email ID Deactivation Process:

- HR Department will share by email the details of resigned employee with IT department indicating date on which e-mail is to be deactivated.
- IT will ensure to deactivate the email id on the mentioned date and will update the requestor via Email.
- In case of requirement of Email forwarding (or e-mail data) of left employee to another employee, request has to submit to CTO after approval from HOD of the concerned department.
- This forwarding of email will be valid for maximum of 90 days of employee last working day. After that email account will be deleted from server along with data unless there is an approval from HOD to continue for a longer period.

Email Usages Guidelines:

Do's and Don'ts for Users

You should :

- Always write well-structured emails and use descriptive but short subjects
- Always check & verify the identity of sender (like someone@abc.com) before replying or taking action on email.
- Always do a spell check before you send out an email.
- Mark emails as important if they really are important.
- Send email to only concerned person(s) and avoid to doing a TO, CC or bcc to persons who are not related to subjected email.
- Set Out of Office autoresponder on if you are on leave or out of office for specific time. This will generate notification to senders that you are unavailable for the period you have mentioned in autoresponder.
- Periodically manage your mailbox by deleting old e-mails, e-mails that are not required, old circulars, cc/ bcc emails etc.
- Use signatures on your e-mail (if you so wish) and signatures can include your name, job title and company name and phone number / address

- Always remember that electronic communications using company's equipment/ domain are considered business communications and all records of such communications are considered business records. Company reserves the right to examine e-mail and reserves the right to use automated monitoring tools to search for words, domains or patterns that may indicate abuse. Such access to e-mail documents will be undertaken only after consultation with Management and will be conducted with due regard for confidentiality.

You should NOT

- Write your email password anywhere at your work place.
- Use your official email on ecommerce websites like Amazon, Flipkart, and Myntra, social website like Facebook or for Subscribing to newsletters.
- Click on any suspicious link received in emails (like click here to win prize or money, click here to change password). These links may contain virus like malware, spam, Trojan that may affect user data & computer.
- Knowingly or intentionally broadcast emails containing false, inaccurate, abusive, offensive or illegal material.
- Write emails in capitals.
- Use Company e-mail id to engage in conduct that violates the Company policies or guidelines.
- Send sensitive & confidential business information outside the domain of company's mail unless until there is clear business need for the same.
- Use e-Mail in any way to conduct any private commercial activity
- Access any other user's e-mail account without that user's explicit permission in writing.
- Send fraudulent, harassing or obscene messages/attachments and/or materials.
- Knowingly or willfully using official email for personal Use.
- Use e-mail for purposes constituting clear conflict of the company's interests or in violation of company's e-mail usage policy or any other policy

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Internet Policy

Objective

The objective of this policy is to provide guidelines for acceptable use of the organization's Internet network to give Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data.

Scope

This policy applies to all employees of the company across all locations

Policy Guidelines

This internet policy covers the activation / deactivation process and Internet Usage Guidelines.

Internet Access Creation Process: -

- All users who are given email access would be eligible for Internet access.
- In case any other employee or third party employees needs internet access or access needs to be provided on any specific machine, user shall have to send a formal request approved by HOD to IT.
- Based on the request, IT department will enable Internet access
- WhatsApp web is not allowed on RTL network unless approved by management
- IT department in consultation with HR will decide the sites permitted for access. In case any special Site / Domain access is required approval from HOD / CTO is required

Internet Access Deactivation Process: -

- The HR department would share information with the IT department when an employee leaves or when deactivation of Internet access for 3rd party is required to be done.
- Based on the request, IT department will disable Internet access

Internet Usages Policy / Guidelines

- Internet facilities provided by company are intended only for achieving business goals and users are expected to make an appropriate and reasonable use of the internet facilities. Appropriate and reasonable use of the internet facilities is defined as use that is consistent

with objectives of the company and with the specific objectives of the project or role for which such use was authorized.

- Management may place any restrictions on the use of the internet including limiting or restricting any access to any individual or group or all users in order to protect the integrity of the internet facilities against unauthorized or improper use, and to protect other users / organizational reputation / information.
- All communication stored on Organization's systems, or received through the internet system are the property of the Organization and organization reserves the right to view them at any time.
- IT Team, through authorized individuals, reserves the right to periodically check and monitor and take any action to protect internet facilities from misuse.
- IT Reserve the right to maintain and monitor the logs of the browsing history of every user who is using company's Internet.
- A visitor or guest user who wants to use the office Internet should be given a Guest login on based the request approved by HOD.
- Users are not allowed to access any prohibited content
- If someone has unintentionally connected to a site / domain that contains harmful content / virus i.e., hacking, gambling, illegal activities, Malware, Virus or any other non-business relevant domains which is not secure then you need to immediately disconnect the PC / laptop from network and inform IT department immediately.
- Following activities are prohibited on the network using any RTL IT resource (Internet link, network, device etc):
    - Using Hotspot or Dongle to access internet on laptop in office
    - Viewing Online movies and similar content, Playing Games, accessing streamlined audio and/or video files, engaging in online chat groups or using system for personal entertainment, personal business or profit, and publishing personal opinions
    - Gaining or attempting to gain unauthorized access to user accounts and passwords whether of internal users or external organizations / individuals;
    - Gaining or attempting to gain access to restricted websites without the permission of the IT Team.
    - Accessing, displaying, uploading, downloading, storing, recording, or distributing any kind of obscene material or pornographic or sexually explicit material
    - Accessing potentially dangerous websites that can compromise the safety of our network and computers.
    - Downloading images, videos, and documents which are not relevant to business.
    - Engaging in any criminal or illegal activity or violating any law.
    - Accessing Dark Net or using software like TOR etc.
    - Uploading or Posting online any Confidential information about RTL (including financial information and information related to customers, business plans, policies, staff, and/or internal discussion) without formal written authorization

- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customer
- Introducing computer viruses, worms, or Trojan horses.
- Using for personal entertainment, personal business or profit, and publishing personal opinions
- Using any peer-to-peer file sharing application like KAZAA, Emule, Bit-Torrents etc

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Laptop and Mobile Device Security Policy

Objective

The objective of Laptop and Mobile device security policy is to help mitigating device security threats and data breaches. Whether devices are personally or company-owned, this policy also aims at making employees aware of the mobile security risks and possible actions that they need to take to mitigate the risks. Mobile device as per this policy would include:

- Laptops
- Tablets / IPADs
- Smartphones

Scope

This policy will apply to both company owned and personal devices used by employees to access company data or any system (for example e-mail, company portal, any software application).

Policy Guidelines

- Users are not allowed to install, uninstall and format the any software (including operating system) on company owned devices. This will be only done by IT department.
- Users should take adequate caution when mobile computing facilities (Laptop, Tablet, Smartphone) are used in public places, meeting rooms and other unprotected areas.
- Users shall ensure that the documents they are studying/drafting on their mobile devices cannot be viewed by anyone else – esp. when using in public places (say while traveling by train or airplane etc).
- All personal devices must be installed with an antivirus before browsing /accessing company data.
- All personal devices must be kept up to date with manufacturer or network provided patches.
- Users must be cautious about the merging of personal and work email accounts on their mobile phone. They must take particular care to ensure that company data is only sent through the corporate email system.
- Mobile devices should not be left unattended. In case a mobile device is lost, it should be immediately reported to IT. An FIR also needs to be lodged by the user. IT team will ensure to change the application password of user profile and wherever possible wipe out company data on mobile phone to prevent data from unauthorised access.

- In case of damage to mobile device or theft, concerned user will be responsible and liable to bear the loss of damage or theft.
- Company or personal laptops must not be checked in airline luggage systems. To avoid damage and theft, these computers must remain in the possession of the traveller as hand luggage.
- Company or personal laptops / Mobile devices should not be left unattended in cars or in train / bus / flight or any public transport.
- Do not keep laptops in the trunk of car as jerks may lead to damage to device.
- In case any users uses personal devices (say personal laptop or PC at home) to access any company data or any system of company for any company related work, he / she would be responsible for the all the software compliance on their personal device – this may include operating system, antivirus and office suite or any other software.
- Users are advised not to load pirated software or illegal content on their personal device (say personal laptop or PC at home).

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Electronic Media Handling & Disposing and Confidential Data Handling Policy

Objective

This policy describes the guidelines for storage and Handling and disposal of electronic media and disposal of paper based confidential records.

Scope

This policy applies to all the IT systems and confidential documents in Rosmerta Group

Policy Guidelines

Disposal of Electronic Media

- Electronic media that need to be disposed of could include old CDs, DVDs, Tapes, USB Pen drives, Hard disks, Digital cameras, Tablets, memory cards etc.
- Many of these could contain sensitive data.
- Electronic information storage media may need to be disposed of due to any reason like
  - Being unusable now and could be scrapped or sold
  - being part of old laptop or PC or server that is being replaced
  - because the media is faulty or has become unusable
  - because the hard drive or equipment has been upgraded
  - part of rental laptop / PC that needs to be returned back or replaced
  - or any other reason
- Any electronic information storage media that needs to be disposed of must be processed by RTL's IT Team for proper erasure or destruction.
- Till the time media is not disposed off, all backup media such as CD/DVD, HDD & Tapes, memory cards, USB etc containing data should be stored in locked almirah / cabinet and should be added in Asset Register. Keys of the almirah should be available with a designated owner mentioned in asset register.
- Prior to sending out for disposal or sale, all media must be formatted and sanitized. Preferably, IT must securely erase data by using Bit-eraser or similar data erasing utility.
- In case of a damaged or inoperable hard drive or media which can not be formatted, IT department must disassemble and mechanically damage or cut the media so that it is not usable by a computer.
- Old CDs, DVDs, Tapes, memory cards etc. must be mechanically damaged or cut so that they are not usable by a computer

- IT Department should maintain documentation of proper sanitization for media and should have a label affixed stating that the media has been properly sanitized.
- CTO needs to ensure that no media goes out of the organization for disposal without removal of data

Disposal of Confidential Documents

- Employees should ensure the documents that are not required are shredded regularly.
- If an employee is not sure if a particular document should be shredded or just disposed off, the rule is "if in doubt, shred".
- RTL has necessary shredding equipment (shredders / multiple blade scissors etc.) which should be used while shredding of any confidential document that is no longer required.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Print Policy

Objective

The objective of this policy is to document guidelines for printing official documents only that are relevant to the day-to-day conduct of business at RTL. This policy aims to ensure that printers are not misused and at the same time we focus on environment by not wasting paper.

Scope

This policy applies to all employees of the company across all locations

Policy Guidelines

- Printers should not be used to print personal documents.
- Avoid printing e-mail messages. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
- Avoid taking printouts wherever possible and rely on electronic version of documents.
- Avoiding printing a document just to see what it looks like. This is wasteful.
- However, if you need to print any document:
    - Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing two PowerPoint slides per page versus only one per page).
    - Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one copy on the printer and use the photocopier to make additional copies.
    - If you print something, please pick it up from printer immediately. If you no longer want any print, please dispose it of appropriately using Shredder.
    - If you come across an unclaimed print job, please handover to the owner or dispose it using Shredder.
    - Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.
    - Color printing is typically not required for most of the official requirements. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.

- Printer paper and Toner cartridges is available with admn department
- If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not “trained” in how to fix the problem, please do not try. Instead, report the problem to IT helpdesk or ask a trained co-worker for help.
- Report any malfunction of any printing device to IT helpdesk as soon as possible.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Secure and Clear Desk Clear Screen Policy

Objective

The objective of this policy is to document protocols that establish requirements on how employees should handle company information and materials within the office. This policy aims to ensure that confidential information and sensitive materials secure when they are not in use.

Scope

This policy applies to all employees of the company across all locations

Policy Guidelines

- Employees are required to secure all sensitive/confidential information in their work space at the end the work day or when they are expected to be away from their work space for an extended period of time. This includes both electronic and physical hard copy information.
- Laptops, workstations. PCs must be locked or logged out or shut down when unattended even during office hours.
- Portable devices like laptops and tablets that may remain in the office overnight must be shut down and stored away.
- Users must shut down their Desktop / Workstation / Printers / Plotters when they leave for the day.
- Mass storage devices such as USB drives or external hard drives must be treated as sensitive material and locked away when not in use.
- Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible. Printed materials must be immediately removed from printers.
- All sensitive documents that need to be destroyed must be placed in the designated shredder bins for destruction, or placed in the locked confidential disposal bins.
- File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
- Passwords must not be written down or stored anywhere in the office
- Keys and physical access cards must not be left unattended anywhere in the office.
- Unattended work areas should be clear of any information whether it is in electronic or paper form.
- Photocopiers shall be appropriately protected for misuse during and after working hours.

- Whiteboards in meeting rooms or conference halls shall be erased as soon as the discussions/ presentations are over.
- If you notice that any of your devices or documents have gone missing, or if you believe your work space has been tampered with in any way, please notify RTL Security immediately along with informing IT helpdesk

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Change Control Policy

Objective

Change Control refers to a formal process for ensuring changes to IT systems are authorized and documented. The objective of change control policy is to ensure that all changes that are made in IT system across RTL are done in a thoughtful way that minimize negative impact to services and customers. Aim is to minimize loss or disruption of service to business support systems and to eliminate any potential conflicts between planned activities and ensure communication to all stakeholders.

Scope

This policy applies to all the changes, upgrades, or modifications to the production environment of any software, hardware or network device. Any modifications, additions or changes to the environmental touch points. Modifications made to non-production systems (such as testing environments with no impact on production IT Services) are outside the scope of this policy.

Policy Guidelines

- Changes to the IT environment may arise due to various reasons such as:
  - Changes in any software application like say new functionalities, version upgrades, bug fixation or because of any business or because of compliance needs or otherwise
  - Upgradation or enhancement or replacement or patching of any software, hardware (server, storage etc.) or network or security device (firewall, switch, router etc.)
  - Environmental changes related to data center, UPS room, Network Room wrt Electrical, access control, Air conditioning, fire extinguishers etc. (whether in-house or hosted at 3rd party)
- **Change Request in case of Software Applications**
  - Either the concerned Business user or Functional Head or any member of IT team can raise a request (ticket) in the IT Ticketing system for any new requirements or modifications in the existing application.
  - This ticket will be considered as initiation of Change Request
  - Functional Head or any member of his team will put in the details of change, efforts required and timelines for the completion of the requirement
  - After approval by Functional head, Business Head and CTO, Ticket will then be forwarded to Management for approval.

- Work will be started post approval.
- After completion of the work a notification via email/ ticketing system will go to the concerned business user regarding UAT (User Acceptance Testing).
- After receiving testing confirmation remarks from user, IT team member will get the approval of Functional head or CTO to move or carry out the changes in production environment.
- After the changes are done in production environment, business user will be informed via email regarding the completion of the requirement and ticket shall be closed by IT.

- **Change Request in case of Network devices, servers and other hardware and any environmental changes**
  - Concerned IT Functional Head or any member of IT team can raise a request (ticket) in the IT Ticketing system for any new addition or upgrade/ change in the existing infrastructure.
  - This ticket will be considered as initiation of Change Request
  - Functional Head or any member of his team will put in the details of change, efforts required and timelines for the completion of the requirement
  - After approval by Functional head and CTO, Ticket will then be forwarded to Management for approval.
  - Work will be started post approval.
  - After the changes are done, IT Functional head will ensure testing either by IIT team members or business users as the case may be and ticket shall be closed by IT.
- CTO will be required to ensure audit of sample change requests on a quarterly basis to check if all changes were properly authorized and tested prior to implementation.
- All changes will be classified into three categories: High, Medium, and Low depending upon the scope and likely impact of the change. In case of changes classified as “High Impact”, concerned IT person will also give the following details to CIO for approval:
  - Impact details
  - Is this change likely to cause downtime and how much
  - If change fails, what is the potential impact (worst case scenario)?
  - What is the Roll-back plan if change fails and likely impact

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Patch Management Policy

Objective

Patch Management Policy is aimed towards managing and mitigating vulnerabilities in company's IT assets through a regular and well-documented patching process. This policy applies to all IT assets of the RTL be it Desktop, Laptops, Servers, network devices, Applications or others.

Scope

This policy applies to all systems (PCs, Servers, Network devices) of the company across all locations

Policy Guidelines

- IT Infrastructure lead needs to ensure that all end user systems and network equipment (PC, Laptops, Switches, Routers, Wi FI access points and other equipment) are regularly patched
- IT Server Admn lead needs to ensure that all servers and storage and related equipment (whether hosted in-house or at third party including Spectra and AWS) are regularly patched
- At the time of Operating system installation (New or re-installation) IT Server Admn lead needs to ensure that all latest patches are applied
- In case of patching of end user IT assets including for like Windows OS, Microsoft or other local applications etc., the patches will be tested by IT Infrastructure lead or his team member in a test environment (of same version) before applying on end users system.
- Patches on the Network devices (Firewall, Router, Managed Switches etc) will be updated only after the recommendation of OEM and after analysing the potential impact.
- In case of Applications like Navision or any Database (liker SQL) or development platforms like dot net etc, the patches will be tested on development or test system (wherever available) before applying on production system. Application backup is mandatory before applying patches.
- In some cases, it may be required to study the impact of patches or firmware update on the dependent devices or on working of application – say Barcode equipment or any printer patch impacting any printing application like DL RC etc. In such cases, patching or firmware upgrade should be done only after confirming from concerned application lead and verifying the end-to-end impact.
- Emergency Security Patching (Zero day) (OS, DB, Application, Network, Server etc.): In case any emergency security patching is recommended by OEM, the same shall be done

with high priority. Before applying emergency security patching same will be tested on test and Development system (whichever is available).

- Till the time there is no patch management software, all patching shall be done manually.
- All patches to be deployed on applications, servers and Network devices must obtain the appropriate change control approval prior to deployment on production systems.
- CTO shall review the status of patch deployment on a quarterly basis and take necessary actions in case of IT assets that are not patched and are still in vulnerable zone.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Vulnerability Assessment (VA) and Penetration testing (PT) Policy

Objective :

Vulnerability assessment (VA) is a systematic technical approach to find the security loopholes in a network or software system. Aim is to find all possible loopholes with the objective that none of the loopholes are missed.

Penetration test (PT) is an approach to actually explore and exploit those vulnerabilities. This process confirms whether the vulnerability really exists and to further prove that exploiting it can result in damage to the application or network.

The purpose of the VA PT Policy is to establish rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. VA/PT should be done for all Information Technology Assets like Firewall, Router, Core Switch, Wireless Controller, WIFI Routers, Servers, Storage, and applications including mobile Apps.

Scope:

The policy applies to all the critical IT assets (Servers, key applications, Core switch, Firewall, Router) of the organization irrespective whether they are hosted in-house or outside.

Policy Guidelines :

- Vulnerability assessment scanning and Penetration testing of the internal network, external network, and all hosted / external / internal applications should be conducted at least once in a year or whenever there is any significant changes to the environment.
- In addition, before launching any new critical application, VA/PT should be carried out.
- VA / PT should be done by a reputed party.
- CTO will designate a person who will be responsible for ensuring the VA / PT is carried out and ensuring that any exploitable vulnerabilities found during a penetration test will have to be corrected and re-tested to verify the vulnerability was corrected.
- A formal report of VA PT and actions taken thereof has to be submitted by CTO to management quarterly.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating

this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy - Incident Management Policy

Objective :

Objective of this policy is to lay down guidelines and actions that need to be taken to respond to and resolve critical incidents by RTL IT Team. This also includes guidelines for detection and communication and other related actions.

Scope:

This Policy is applicable to all IT hardware and software assets in the organization. IT Assets include:

- Applications – Email, ERP, HSRP, and all other software applications
- Network and Security Devices - Firewall, Wi-Fi, Switches, Network Printers
- Data Centre Equipment - Servers, Storages, Chassis (whether hosted in-house or at Spectra or AWS or any other location)
- End User Asset- Desktop, Laptop, Workstation & printers

Policy Guidelines :

- Any Incident that impacts IT services may come to knowledge of IT either when informed by end user or by any member of IT Team or third party support team or based on analysis of logs or review of daily checklists, system performance monitoring etc or any system generated alert or thru Ticketing System.
- The Role of IT Team in case of any incident that impacts IT services includes but is not limited to
    - Analysis and identification of the cause of the incident
    - Planning and Implementation of remedies to resolve the issue (wherever possible) and to prevent recurrence
    - Assessment of the impact of the incident, especially in cases of breaches of confidentiality or privacy
    - Collection of audit trails and similar evidence
    - Reporting the incident to management and if applicable also to authorities like CERT in
- All the incidents need to be logged in the IT Ticketing System (by user or IT person as the case may be)
- Based on severity and priority of incident, all incidents should be categorised as High (P1); Medium (P2) and Low (P3)
    - High (P1): These include incidents like Fire incident, Critical Systems Down,

Business critical applications not accessible, where there is direct impact on production or sales; major IT security incident etc.

- Medium (P2): These include incidents that have significant impact but may not be not a production or sales outage but affects user's experience significantly (e.g., slow performance), virus attack on some individual machine etc.
- Low (P3): These include incidents that do not interrupt group of users or the business but individual computer, printer etc
- Annexure 1 at the end of this policy gives the Incident Management Response and Resolution Time based on Severity Ratings
- Annexure 2 at the end of this policy gives details of Escalation Matrix and Contact Details for various kinds of incidents. This should be updated every month by IT team to ensure that numbers and names are current.

- The incident call will be assigned by the concerned Functional Head or Manager to relevant Engineer (depending upon the nature/type of call logged and its severity)
- The Engineer will also get an information of the assigned call (i.e., Name and contact number of User / details of system and type of issue reported)
- After receiving details of incident, IT engineer will start working on call based on the priority of the call/User.
- The Engineer will analyse and identify the cause of the incident
- IT team will plan and implement remedies to resolve the issue (wherever possible) and to prevent recurrence.
- IT Engineer will update the user about the closure date (day/time) to fix the incident reported.
- Based on the priority of call IT Engineer will arrange standby option for reported issue.
- Concerned IT Functional Head / manager will also assess the impact of the incident, especially in cases of breaches of confidentiality or privacy
- Evidences (wherever possible) will be collected and stored in a secured location by IT team and should be readily available with the team so that same can be produced in support of any legal or disciplinary actions if needed.
- An incident will be closed once the issue is resolved and the user has acknowledged the resolution.
- Once the Incident is completely addressed the following information should be documented in format as given in Annexure 3.
    - Incident details
    - Time Incident reported.
    - Severity / Impact
    - Time Incident closed.
    - Root Cause Analysis.
    - Corrective Actions taken
    - Corrective measures taken to prevent recurrence.
    - Evidences collected. (If possible)

    - Lessons Learnt
    - Any disciplinary/legal action taken. (If required)
- CTO will be responsible for reporting the incident to management and if applicable also to authorities like CERT in

- **Reporting Incidents to CERT IN :**

  As per Indian Computer Emergency Response Team (CERT-IN), it is mandatory that all cybersecurity incidents in relation to cybersecurity incidents need to be reported to the CERT-IN within six hours from incident identification/notification. CTO will be responsible for all reporting to CERT IN and will be designated as Point of Contact (POC) to liaison with CERT-IN. Detailed guidelines are given in Annexure 4. The guidelines in Annexure 4 are applicable to all IT incidents (as per CERT-IN List) at any part of the Organization across all offices and factories.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

Annexure 1

Incident Management Response and Resolution Time based on Severity / Priority Ratings

Severity / Priority	Response / Resolution time	Details
High (P1)	Response Time: 15 minutes Resolution Time: 2 hours	A problem which has mass impact to users. A problem that impacts Production or Dispatch A problem related to system of Chairman, members of management and senior leadership
Medium (P2)	Response Time: 30 minutes Resolution Time: 4 hours	A problem in which system (Server /application) is running but slow performance is observed or it impacts a particular system or user.
Low (P3)	Response Time: 30 minutes Resolution Time: 1 Day / Best Effort basis	A problem related to the installation, movement, upgrade/ changes in hardware, software, network etc.

Annexure 2

Incident Management Reporting – Escalation Matrix and Contact Details

Area	Level 1 Escalation Name – Designation e--mail ID Mobile Number	Level 2 Escalation	Final Escalation
IT Infrastructure - Spectra			CTO
IT Infrastructure – AWS			CTO
IT Infrastructure – End users			CTO
HSRP Applications			CTO
VTS Applications			
Digital Applications			
DLRC Applications			
ERP Applications			
Other Applications			

Annexure 3

Format for Root Cause Analysis

Report Prepared By:	**Incident Reference Number**
Date of Report:	**Incident Reported by**
Date of Occurrence of Incident:	**Time of Occurrence of Incident:**
Date of Closure of Incident:	**Time of Closure of Incident:**
Place of Occurrence of Incident:	**Severity of Incident :**
Description of Incident:	
Impact of Incident:	
Root Cause of Incident:	
Corrective Actions Taken:	
Preventive Action for future:	
Key Learnings:	
Any Disciplinary / Legal Action:	
Evidences Collected (If any)	

Annexure 4

Reporting Incidents to CERT IN Policy

Background

On 28 April 2022, the Indian Computer Emergency Response Team (CERT-IN), Issued directions mandating that all cybersecurity incidents in relation to cybersecurity incidents need to be reported to the CERT-IN within six hours from incident identification/notification.

A computer security incident is any adverse event whereby some aspect of a computer system is threatened viz. loss of confidentiality, disruption of data or system integrity, denial of service availability. Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents. By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyse them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the Incidents in future.

Type of incidents that need to be reported

- As per CERT-IN directives, we need to report following types of incidents:
    - Targeted scanning/probing of critical networks/systems
    - Compromise of critical systems/information
    - Unauthorized access of IT systems/data
    - Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites etc.
    - Malicious code attacks such as spreading of virus/worm/Trojan/Bots/Spyware/ Ransomware/Cryptominers
    - Attack on servers such as database, mail and DNS and network devices such as routers
    - Identity theft, spoofing and phishing attacks
    - Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
    - Attacks on critical infrastructure, SCADA and operational technology systems and wireless networks
    - Attacks on applications such as e-governance, e-commerce etc.
    - Data breaches
    - Data leaks

- Attacks on Internet of Things (IoT) devices and associated systems, networks, software, and servers
- Attacks or incidents affecting digital payment systems
- Attacks through malicious mobile apps
- Fake mobile apps
- Unauthorised access to social media accounts
- Attacks or malicious /suspicious activities affecting cloud computing systems/ servers/ software/ applications
- Attacks or malicious /suspicious activities affecting systems/servers/networks/ software/ applications related to Big Data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing,
- Attacks or malicious /suspicious activities affecting systems/servers/software/ applications related to AI and ML

Who will report the incident

- As per CERT-IN, a Point of Contact (POC) needs to be designated to liaison with CERT-IN. The details of the POC (Name; Designation; Organisation name; Office address; Email ID; Mobile number; Office phone and Office fax) need to be sent to CERT-IN and need to be updated from time to time.
- CTO will act as designated POC for CERT-IN
- Any change in the POC will be communicated to CERT-IN within 3 working days of change
- All communications from CERT-IN shall be sent to the designated POC.

Timelines of reporting an incident

- All incidents will need to be reported to CERT-IN within six hours from the occurrence of the incident or of the incident being brought to the SPOC's notice.

Contents of Incident Report

The following information (as much as possible) may be given while reporting the incident.

- Summary of incident
- When was the incident detected (date and time)?
- How was the incident detected?
- Which is affected by the incident, IPs or URLs?
- Details of the affected system or service (location, platform, details of security audit done)
- Details of incident investigation (if any)

- Details of mitigation action (if any)
- Details of impact
- Incident reporter (name, phone number, e-mail, and address)
- Details of Contact Person for the incident (name, phone number, e-mail & address)
- Any other relevant information

Incident reporting format is given at the end of this policy.

How and where to report an incident

- Incidents can be reported to CERT-IN via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969).

Other CERT-IN directives

As per CERT-IN directives, we need to adhere to the following:

- Enable logs of all their Information and Communication Technologies (ICT) systems.
- Retain logs for 180 days.
- Synchronise time with National Informatics Centre's Network Time Protocol. Organisations must connect to the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems' clocks.
    - National Informatics Center(NIC): Samay1.nic.in, samay2.nic.in
    - National Physical Laboratory: time.nplindia.org

IT Policy - Third party Access Policy and Confidentiality Agreement (NDA)

Objective :

The objective of this policy is to restrict the access of Third party employees including visitors and other guests to the company's IT network and other IT resources in order to prevent the spread of viruses, spywares or malwares via any infected laptop of the guest / visitor and to check unauthorized access to sensitive areas of the IT Infrastructure. For the purpose of this policy, guests are categorized as

a) Visitors (who visit RTL's premises for some meeting for a limited period of the day and need access to the internet or any IT related facility of RTL for few hours).and
b) Third party Employees (Employees of 3rd– For example if some 3rd party people are stationed at RTL's premises for ERP Support etc.).

Scope:

The policy applies to all Visitors (who visit RTL's premises for some meeting for a limited period of the day) and need access to the internet or any IT related facility of RTL and Third party Employees stationed at RTL's premises.

Policy Guidelines :

For Visitors:-

- RTL Employee who invites the visitor or whom the visitor is visiting to; is responsible and will be single point of contact for each and every activity of the visitor inside the company's vicinity.
- Visitor should always wear Visitor badge while inside the vicinity and should carry visitor slip issued to him by reception staff and get the slip signed by the employee he/she visits.
- In case the visitor requests for connecting his/her laptop to internet, the RTL Employee will have to get this request approved by HOD with details including Visitor name, Mobile number and duration for which access is required and send the approval mail to IT Team for further processing or log a ticket in IT Helpdesk Ticketing software and attach the approval mail to it.
- After validating the approval, IT team would provide the necessary access.
- Visitors will not have any access to Shared drives, printers, servers and any other network resources.

- Internet access provided to the visitor will be for limited period (maximum 9 hrs) and will be deactivated at the end of the period / end of day.
- Visitors will not be allowed to plug in their device to local network and all access will be provided via Wi-Fi only.

For Third party Employees:-

- Any Third party Employees stationed at RTL will be the responsibility of the concerned Manager / process owner in whose area they are working.
- Concerned Manager / process owner will get the approval from HOD for issuing the access control card to Third party Employees.
- In case any Third party Employee requests for connecting his/her laptop to internet, the Manager / process owner will have to get this request approved by HOD with details including Third party Employees name, Mobile number and nature and duration and applications / devices for which access is required and send the approval mail to IT Team for further processing or log a ticket in IT Helpdesk Ticketing software and attach the approval mail to it.
- After validating the approval, IT team would provide the necessary access.
- Access provided to the Third party Employees will be for the duration and scope for which access has been approved and will be deactivated at the end of the period.
- In case any Third Party Employees needs access to any shared drive, printer, server, application or any other IT resources including access to Network room there has to be a formal NDA / Confidentiality agreement between RTL and the Third party employee (or the organization from whom the person is deployed) will be signed before giving any access to any RTL System & Applications. NDA format as per Annexure.
- Access will not be provided on Third Party's laptop but will be provided only by giving them access to RTL PC / laptop and not on their laptop.

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

Annexure 1 - Format of NDA / Confidentiality Agreement

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (hereinafter referred to as the **'Agreement'**) is executed on this ……. day of ……., 202X, by and between:-

Rosmerta Technologies Limited (CIN:xxxxxxxxxxx)**,** a company incorporated & registered under the Companies Act, 1956 having its registered office at xxxxxxxxxxxxxxxxxxxxxx. (hereinafter referred to as **'RTL',** which expression shall, unless repugnant to the context or meaning thereof, mean and include its administrators & permitted assigns), of the **One Part;**

and

…… (CIN : ……)**,** a company incorporated & registered under Companies Act, 1956, having its registered office at …… (hereinafter referred to as '……**',** which expression shall, unless repugnant to the context or meaning thereof, mean and include its administrators & permitted assigns), of the **Other Part.**

RTL and ……. are hereinafter also collectively referred to as **'Parties'** and individually as **'Party',** unless repugnant to the context.

Whereas RTL is, inter-alia, engaged in the business of e-governance services and manufacturing & selling of automotive components.

Whereas ……. is engaged in the business of ……

Whereas pursuant to the negotiations between the Parties and for the purpose as stated supra, it is contemplated that RTL shall disclose to the other Party certain information & data, which are non-public, confidential and of proprietary nature.

Whereas Parties are desirous of entering into this Agreement to protect such information from being infringed / disclosed.

NOW THEREFORE, intending to be legally bound, the Parties to this Agreement agree as follows:

1. DEFINITIONS AND INTERPRETATION:

In this Agreement, the following defined terms shall be interpreted to carry the meaning set

forth in this Clause:-

1.1 **"Confidential / Proprietary Information"** shall mean and include sharing of information of RTL for the any activity related to Project (as defined in Clause 1.5 hereunder) & thereafter implementation thereof.

The Confidential Information also includes the information of RTL, which is not in the public such as corporate strategies, data, records, databases, computer programs, software applications, data lying on servers and trade secrets, discussions on zoom calls (whether recorded or unrecorded), general business information or market information, marketing, sales, customers', suppliers', consulting relationships' information received or obtained before, on or after the date of this Agreement, whether or not marked or designated as 'in written, oral or otherwise, including electronic or optical data storage and retrieval mechanisms, and including all forms of communication, including but not limited to physical demonstrations, in-person conversations and telephone conversations, and other means of information sharing such as facility tours, regardless of whether any such information is protected by applicable trade secrets or similar laws, and any analysis, compilations, reports, memoranda or studies with respect to such information prepared, but excluding information which : -

i. is or becomes publicly available (other than as a direct or indirect result of any breach of this Agreement); or
ii. is known to the Receiving Party before the date it is disclosed by the Disclosing Party or is obtained by the Receiving Party after that date from a third person who, insofar as is known to the Receiving Party, is not prohibited from transmitting the information by a contractual, legal or fiduciary obligation to the Disclosing Party provided the Receiving Party shall substantiate the same fact to the Disclosing Party without any delay;
iii. is independently developed by the Receiving Party without having any reference of Confidential Information of Disclosing Party provided the Receiving Party shall substantiate the same fact to the Disclosing Party without any delay.

1.2 **"Disclosing Party"** means the party which shall disclose the Confidential / Proprietary Information to the other Party, for the purpose of this Agreement;

1.3 **"Receiving Party"** means the party to whom the Confidential / Proprietary Information shall be disclosed by the Disclosing Party for the purpose of this Agreement;

1.4 **"Representatives"** mean the directors, officers, employees, agents, attorneys, accountants, consultants, technical personnel, financial advisors and other authorized

persons of the Receiving Party and of its affiliate as the case may be.

1.5 **"Project"** means and includes all activities including the negotiations, deliberations, talks, meetings and implementation / support activities

2. CONFIDENTIALITY UNDERTAKING:

2.1 In consideration of the Disclosing Party disclosing Confidential / Proprietary Information to the Receiving Party, the Receiving Party undertakes to the Disclosing Party that the Receiving Party shall: -

i. not disclose or release the Confidential / Proprietary Information to any third party including competitors. However, the Receiving Party shall disclose or release the Confidential / Proprietary Information only to its Representatives to the extent relevant and required for the purpose of this Agreement and the Receiving Party shall ensure that such Representatives are restrained from disclosing or releasing the Confidential / Proprietary Information of the Disclosing Party to any third party and are bound by the confidentiality or non - disclosure provisions of this Agreement;

ii. be responsible & / or liable for any disclosure or release of Confidential / Proprietary Information by its Representatives in violation of this Agreement and shall enforce confidentiality obligations against its Representatives with respect to the Confidential / Proprietary Information;

iii. not use any Confidential / Proprietary Information for its own benefit or for the benefit of others including competitors, in any manner whatsoever in India & / or rest of the world;

iv. not to commercially exploit the Confidential / Proprietary Information of the Disclosing Party;

v. hold in confidence all Confidential / Proprietary Information received from the Disclosing Party pursuant to this Agreement;

vi. protect the Confidential / Proprietary Information and take all safeguards necessary for the same from being disclosed, destroyed, tampered, copied, conveyed or communicated and accessed by any third party;

vii. not do engineering / reverse engineering of the Confidential / Proprietary Information of the Disclosing Party except for the implementation & completion of the Project as agreed upon between the Parties as stated supra;

viii. shall not violate the principles of infringement and passing off;

ix. not file or attempt to file any patent or design or trademark or domain name application, directly or indirectly, whether in its own name or in the name of its associates / affiliates etc., based upon or disclosing any of Disclosing Party's Confidential / Proprietary Information in India & / or rest of the

world;

x. not use the Confidential / Proprietary Information for any purpose other than in relation to the Project;

xi. take all reasonable precautions in handling, evaluating, using and disposing of the Confidential / Proprietary Information, and the Receiving Party shall be solely responsible & liable for any damages arising from any failure to do so; and

xii. return the whole such information if the purpose for which the same is parted with does not mature or completed.

2.2 The Receiving Party shall promptly notify the Disclosing Party if it becomes aware of any breach of confidence by any person, firm or corporation to whom it has divulged all or any part of the Confidential / Proprietary Information or who becomes aware of it in an unauthorized way, and shall give the Disclosing Party all reasonable assistance in connection with any proceedings which the latter may institute against such person, firm or corporation to prevent disclosure of such Confidential / Proprietary Information.

3. RETURN OF CONFIDENTIAL / PROPRIETARY INFORMATION:

At the time of expiration / termination of this Agreement or in the event the Project for which the Confidential / Proprietary Information is disclosed to the Receiving Party does not mature or completed or upon the receipt of a written request from the Disclosing Party, the Receiving Party shall:-

i. return promptly to the Disclosing Party the Confidential / Proprietary Information which is in the Receiving Party's possession or control or in the possession or control of the Representatives & any such persons to whom Confidential / Proprietary Information was required to be disclosed for the implementation of the Project; and

ii. expunge immediately all Confidential / Proprietary Information from any computer, word processor or similar device into which it was programmed by the Receiving Party or on its behalf or by its Representatives or on their behalf or by such persons to whom Confidential / Proprietary information is disclosed or on their behalf & confirm the same in writing to the Disclosing Party.

4. PUBLIC ANNOUNCEMENTS:

Neither Party shall make any public announcement in relation to the Project save where either Party reasonably determines in writing that a public announcement is required by any applicable regulation and provided that such announcement shall be made only after reasonable consultation with the other Party and after taking into account the other Party's reasonable written request with the written consent as to timing and content.

5. RELIEF:

The Receiving Party acknowledges that damages alone would be the inadequate remedy for breach of this Agreement and without prejudice to any other rights and remedies otherwise available to the Parties, the Receiving Party agrees that injunctive relief would be a more appropriate remedy.

6. INTELLECTUAL PROPERTY RIGHTS:

All Confidential / Proprietary Information furnished by the Disclosing Party to the Receiving Party & / or its Representatives shall remain the exclusive property of the Disclosing Party.

The sharing / exchange / disclosure of Confidential / Proprietary Information hereunder shall not in any manner be construed, whether expressly or by implication, estoppels or otherwise, as granting / acquiring the Receiving Party a license, interest or right in or under any patents, know how, copyrights, drawings, designs or trademarks or domain names owned and controlled by the Disclosing Party and its holding, subsidiary and affiliates, present or future. The Disclosing Party makes no representation or warranty in this Agreement, express or implied, with respect to the accuracy, completeness or utility of any Confidential / Proprietary Information provided pursuant to this Agreement.

Further, the Intellectual Property Rights as arise in relation to the Project shall exclusively belong to RTL.

7. WAIVER:

No failure or delay by the Parties in exercising any right, power or privilege under this Agreement will operate as a waiver of it, nor will any single or partial exercise of it preclude any further exercise of any such right, power or privilege.

8. SEVERABLE:

The provisions of this Agreement shall be severable in the event that any of the provisions are held by a court of competent jurisdiction to be invalid, void or otherwise unenforceable and the remaining provisions shall remain enforceable to the fullest extent permitted by law.

9. INDEMNITY:

If this Agreement is breached by the Receiving Party & / or its Representatives, the Receiving

Party will fully indemnify, protect, defend and hold harmless the Disclosing Party from and against any and all actions, claims, demands, proceedings, liabilities or judgments and any and all losses, damages, costs, charges and expenses of whatever nature and in whichever jurisdiction which may be instituted, made or alleged against, or which are suffered or incurred by the Disclosing Party and which relate to or arise directly & / or indirectly from any such breach.

10. NOTICES:

All notices and demands of any kind or nature which either Party to this Agreement may be required or may desire to serve upon the other Party in connection with this Agreement shall be in writing and may be served personally or by e-mail (at following designated e-mail IDs) or by prepaid registered post or by private reputed courier service, in either case to the address set forth in this Agreement: -

If to RTL : .....

If to ..... : .....

11. ASSIGNMENT:

Neither Party shall assign or transfer any rights or obligations under this Agreement without the prior written consent of the other Party and any attempt of assignment or transfer without such consent shall be void.

12. COUNTERPARTS:

This Agreement may be executed in any number of counterparts, and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

13. MODIFICATION:

No modification, variation or amendment to this Agreement will be effective unless made in writing and signed by duly authorized representatives of each of the Parties.

14. DISPUTE RESOLUTION:

In case of any dispute arising between the Parties at any point of time, the Parties shall refer the dispute to a single arbitrator appointed with the consent of both the Parties. If the Parties fail to have consent for a single arbitrator, then both Parties shall appoint one arbitrator each and

the two appointed arbitrators shall appoint the third arbitrator, who shall act as the presiding arbitrator. The arbitral proceedings shall be conducted under the provisions of Arbitration & Conciliation Act, 1996 and rules thereof. The language of the arbitral proceedings shall be English. The Parties shall bear the arbitration expenses in 50:50 ratio. Either Party shall bear its counsel's fee. The place of arbitration shall be at Delhi in India.

15. GOVERNING LAW & JURISDICTION:

This Agreement will be governed by and construed in accordance with the laws of India and each Party submits to the exclusive jurisdiction of the Courts in Gurgaon in India.

16. SURVIVAL:

The obligation to keep the Confidential / Proprietary Information furnished by the Disclosing Party to Receiving Party & / or its Representatives as confidential shall survive the early termination / expiry of this Agreement.

17. TENURE & TERMINATION:

The tenure of this Agreement shall remain in full force for the period of 3 years from the date set forth on the first page hereof, and if the Project for which the Confidential / Proprietary Information is shared is not achieved within the above given period, the tenure of this Agreement may be extended by the mutual consent of both the Parties in writing.

This Agreement may be terminated by either Party by giving prior written notice of 30 days to other Party.

IN WITNESS WHEREOF, both the Parties hereto have executed this Agreement on the day, month and year first above written

For Rosmerta Technologies Limited	**For .....**
Sign :	Sign : .....
Name :	Name : .....
Designation :	Designation : .....

IT Policy - Baseline Hardening Policy

Objective

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and reducing the system's attack surface by removing unnecessary programs, accounts, applications, ports, permissions, access, etc.

The objective of this policy is to ensure secure use of Company's IT assets are hardened so as to reduce the vulnerabilities that can be exploited by hackers.

Scope

This Policy is applicable to all hardware and software assets in the organization including those hosted at Spectra or AWS or any other provider viz.:

- End user equipment and applications – Desktops, Laptops, Email, Applications (Both in house and bought)
- Network and Security Devices – Firewall, Wi-Fi, Switches, Network Printers, Other devices
- Data Centre Equipment – Servers, Storages, Other Equipment

Policy Guidelines

- Always harden all IT equipment before connecting them to the internet or to external networks or before handing them over to users
- Avoid installing unnecessary software on servers
- Enforce secure passwords and Two factor authentication for all logging on to servers, storage and critical networking equipment
- Regularly Remove unused accounts
- Ensure super user and administrative shares are properly set up, and that rights and access are limited in line with the principle of least privilege
- Never test hardening on production servers
- Give remote access on VPN only
- Follow all guidelines as below at all times

Physical Security:

- Restricted Access: Place Servers, Storage, Controllers, Routers, Firewall and other

equipment in secure, access-controlled rooms with environmental controls (temperature, humidity). Restrict physical access to the location using biometric locks, card readers, and surveillance cameras to monitor access.

- Inventory: Maintain an up-to-date inventory of servers, storage and all other equipment and their locations.

Secure Configuration:

- Change Default Credentials: Change default passwords for all devices immediately after installation.

Access Control:

- Strong Authentication: Enforce strong password policies and implement multi-factor authentication (MFA) where possible.
- Least Privilege Principle: Limit user privileges to the minimum required for their roles.
- Role-Based Access Control (RBAC): Implement RBAC to restrict access based on job roles.
- Disable Default Accounts: Disable or rename default accounts (e.g., administrator, guest) to prevent unauthorized access.
- Use NTFS (Windows) or Ext4 (Linux): Implement file and folder permissions to restrict access to authorized users only.

Operating System and Database Security:

- Patch Management: Keep the OS and software up-to-date with the latest security patches.
- Minimal Installation: Install only necessary components, reducing the attack surface.
- Remove Unnecessary Services: Disable or remove unnecessary services, applications, drivers, file sharing, libraries, software, services, and functionality
- Regular Updates: Keep firmware, drivers, and management software up to date. Apply patches and security updates promptly.

Network Security:

- Firewall Configuration: Enable and configure firewalls to allow only essential incoming and outgoing traffic.
- Secure Remote Access: Use secure protocols (e.g., SSH, VPN) and change default ports for remote access.
- Intrusion Detection/Prevention Systems (IDS/IPS): Implement IDS/IPS to monitor and block suspicious network activities.
- Network Segmentation: Isolate Server room traffic from other network traffic. Use VLANs

to segregate traffic.

- Ensure firewall / core switch , router , edge switch , WLC , Access Point are properly configured and that all rules are regularly audited
- Regularly apply any updates or patches
- Block any unused or unneeded open network ports
- Disable and remove unnecessary protocols and services
- Implement access lists

Logging and Monitoring:

- Enable Logging: Enable and configure system logging to track security events and activities. Log all activity, errors, and warnings; implement privileged user controls.
- Enable Audit Trail: Enable auditing features to log access and configuration changes.
- Centralized Logging: Centralize logs to a secure, remote server for analysis and monitoring.
- Real-time Monitoring: Implement real-time monitoring to detect and respond to security incidents promptly.

Data Encryption:

- Data-at-Rest Encryption: Use storage-level encryption solutions to encrypt data at rest within the SAN / server.
- Data-in-Transit Encryption: Ensure data is encrypted while being transmitted between SAN devices / servers.

Application Security:

- Application Whitelisting: Allow only approved applications to run on the server.
- Regular Updates: Keep all applications and server-side scripts updated with the latest security patches.
- Restrict access to applications based on user roles where ever possible (as per application control Policy)
- Remove all default passwords
- Set Application passwords including password rotation, length, etc. as per the password policy.
- Regularly inspect integration with other applications and systems, and remove, or reduce unnecessary integration components and privileges

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating

this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the policy at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

IT Policy – Application Development

Objective:

This policy defines the steps for both new application development as well as change in an existing application.

Policy Guidelines

- First step in Application Development or changes is to create a Business Requirements Document. Business Requirements Document (BRD) is a formal document that describes the high-level business requirements for an IT project. It serves as a foundational reference point that outlines the business needs, objectives, and scope of an IT project. It acts as a bridge between business stakeholders and the IT team, ensuring that everyone understands and agrees on the project's goals and scope.
- The key objectives of a Business Requirement Document are:
    - To build consensus among stakeholders.
    - To communicate the business needs, the customer needs, and the end result of the solution that must satisfy business and customer needs.
    - To determine the input to the next phase of the project.
- BRD should be prepared by concerned IT team member (business analyst or project manager as the case may be) in collaboration with key business stakeholders.
- BRD should contain the following information:
    - Project Scope: A clear description of what the project will and will not include.
    - Key Stakeholders: List the key stakeholders for the project
    - Business Objectives: The overarching goals and objectives the project aims to achieve.
    - Requirements: Detailed descriptions of the user requirements – both functional and Non-Functional Requirements (if any) like Performance, security, and any other expectations.
    - Assumptions and Constraints: Any assumptions made in the requirements and any constraints that may affect the project.
    - Project Timeline: High-level project timeline and milestones.
    - Risks and Mitigations: Any potential risks and how they can be addressed.
- Template of the BRD enclosed in Annexure.
- BRD should be reviewed and signed off by key stakeholders, including project sponsor, business owner, CTO and IT functional head and any other relevant stakeholder. Their approval indicates their agreement with the documented business requirements and serves as a basis for further project planning and development.
- Once signed, copy of BRD should be circulated among all the key stakeholders

- Any revision in scope of the project or any functionality has to be approved by all the stakeholders who signed the BRD.
- Once signed Business Requirements Document (BRD) is received, a feasibility and impact study needs to be done to analyse:
    - Manpower effort required
    - Hardware and Software components required (if any)
    - Cost of development/change (In case to be done externally)
    - Impact on existing systems (if any)
- Business / User requirements need to be then converted into a detailed specification document – User Requirement Specification document (URS) by the functional Head. This document should describe, in business terms, about the functionality which the application shall provide and it should also include design details such as interfaces with other systems and data requirements.
- While coding for applications, the following coding practices must be referred to
    - The code must be easily understandable, reusable, secure and easy to maintain
    - The code must be well-laid out and commented.
    - Standardized naming and definition of data elements must be used
    - Guidelines for Security of Web Applications should be followed
    - Multiple-line statements, complicated logic and unstructured code must be avoided to ensure ease of debugging
    - As far as possible, on-line and context sensitive help should be provided in software products.
- In order to ensure that the software solution performs as intended and delivered defect-free prior to installation & commissioning, it shall be tested and testing results need to be documented. Following kinds of testing needs to be done (as applicable)
    - Unit testing: In this case, focus is on individual units of code (functions, classes) to ensure they work as expected. Developers need to write unit tests themselves.
    - Integration testing: Here the aim is to tests how different software modules interact with each other. This is crucial to identify issues how data flows between various modules and with other systems as applicable. Developers need to write integration test scenarios themselves.
    - Functional testing: In this, team needs to test software functionality against requirements. Aim is to ensure the software performs actions according to its intended purpose. This has to be done by core users.
    - User Acceptance Testing: This is formal testing that needs to be done by users or stakeholders to validate if the software meets their needs and acceptance criteria.
    - Performance testing: In case of software that would involve high transaction volumes, performance testing needs to be done to assess how the software behaves under load (e.g., many users, large data volume). This would help identify bottlenecks and ensure the software can handle real-world usage.

    - Regression testing: This is required in case of changes in existing systems Aim is to ensure new changes haven't introduced bugs in existing functionalities.
- In case of critical software, external PT (Penetration Testing) / VA (Vulnerability Assessment) or Third Party Code review can also be done.
- Functional heads need to ensure that all test results are documented and signed by concerned people who have done testing

Violation of Policy

The company takes serious note any violations of the policy. Any employee found violating this policy will be subject to disciplinary action as determined by Head of Department or HR.

Policy Review / Amendments / Modifications / Withdrawal

This policy will be reviewed from time to time, and the company reserves the right to modify/amend/alter and/or withdraw the SOP at its discretion.

In case of any doubt, the interpretation of above terms by the CTO shall be final.

Annexure 1

Template for BRD

RTL	Business Requirement Document
Project Name / Brief Description:	
Project Owner:	IT Owner:
Project Sponsor:	IT Sponsor:

	Prepared By	Reviewed By	Approved By		
Name					
Designation					
Signature					
Date					

1. Introduction

1.1 Purpose: Describe briefly the purpose of the project.
1.2 Stakeholders: Identify the main stakeholders and their roles.

2. Project Overview

2.1 Key Objectives: List the overarching goals and objectives of the project.
2.2 Scope: Define the scope of the project and the key objectives.
2.3 Key Requirements: List the specific requirements or preferences expressed by stakeholders.
2.4 Project Timeline: Provide an initial timeline for the project.

3. Assumptions and Risks

3.1 Assumptions and Constraints: Mention any assumptions and constraints that affect the project.

3.2 Risks and Mitigations: Identify potential risks and how they will be addressed.

4. Sign-off

4.1 Provide space for stakeholders to sign off on the BRD, indicating their agreement with the documented requirements.

Appendices (if necessary)

A.1 Include any additional information, supporting documentation, or references.
A.2 Glossary : Define any technical terms or acronyms used in the document