P-PL02 Attendance Policy

1. Purpose

The purpose of this policy is to set forth guidelines for handling employee absences and tardiness to promote the efficient operation of the company and minimize unscheduled absences.

2. Scope

2.1 Employment type

This policy is applicable to

- [x] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- This policy is applicable for both “working from office” and “remote work” models.
- This policy is not applicable for absences due to planned leave.

3. Policy Statements

- Punctual and regular attendance is an essential responsibility of each employee at 99x.
- Working hours are from 8.00 a.m. to 5.00 p.m. or 9.00 a.m. to 6.00 p.m..
- Employees are expected to report to work as scheduled, on time and prepared to start working.
- All employees should record in and out times.

- It is the employees' responsibility to ensure that they are at work for 9 hours including one hour lunch break and the given flexibility is not misused.
- Late arrival, early departure or other unplanned absences from scheduled hours are disruptive and must be avoided.

Absences

- If the employee is unable to report to work due to sickness or any other emergency, the Team Lead/Supervisor must be kept informed before 10.00 a.m. on the first day of absence.

Tardiness

- If the employee is reporting to work late due to sickness or any other emergency, the Team Lead/Supervisor must be kept informed. This notification does not excuse the tardiness but simply notifies the stakeholders that a schedule change may be necessary.
- Employees are expected to return from scheduled breaks on time.

Early departures

- Employees who must leave work before the end of their scheduled shift must notify the Team Lead / Supervisor immediately.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR05 Attendance Process

6. Classification

.

☐ Sensitive

☐ Confidential

☑ Restricted

☑ Internal

☐ Public

L-PL15 Information Systems Audit Policy

1. Purpose

Regular audits help to ensure that controls are sufficient and effective at providing information confidentiality, protecting Personally Identifiable Information (PII), ensuring system availability, and fostering a higher degree of data integrity. This policy sets forth 99x's practice regarding information system related audits.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy covers all information systems of 99x including software and hardware systems.
- This policy covers all organizational functions except Finance.

3. Policy Statements

- Following information system audits are applicable.
  - Internal audits.
  - External audits.
  - Third-party audits.
  - Internal VAPT
  - External VAPT
  - Non-functional developer testing.
  - Non-functional QA testing.
  - Non-functional production testing.
- These audits shall be conducted as planned activities according to a schedule.
- Audit findings shall be recorded and assigned back to the relevant auditee. Follow up audits shall be conducted to verify the implementation of the findings.

Internal Audits

- Internal Audits shall be conducted to verify the conformity to all compliance requirements of,
  - Departments.
  - Customer Projects. Internal audits conducted on customer projects are called Product Health Reviews.

- Internal audits shall be conducted by 99x employees who are trained on conducting such audits.
- Internal Audits shall be independent and shall not cover the own implementations of the auditor.
- There shall be two internal audit cycles per year.
- When conducting the audits, the internal auditors will get access only up to the level they have clearance for access.

External Audits

- External audits shall be conducted to verify the conformity to the relevant ISO standard requirements as specified in the L-PL01 Integrated Management System Policy.
- A qualified third-party service provider shall be engaged in conducting external audits.
- There shall be two external audit cycles per year.
- When conducting audits, the external auditors will get access to any information required.

Third-Party Audits

- Third-party audits shall be conducted on selected suppliers to verify the conformity of their internal processes to relevant ISO standards.
- A qualified third-party service provider shall be engaged in conducting third-party audits.
- Third-party audits shall be conducted as and when they are required.

Internal VAPT

- Internal VAPT shall be conducted to uncover any technical vulnerabilities of information systems.
- Internal VAPT shall be conducted by 99x employees who are trained on conducting such audits.
- There shall be two internal VAPT cycles per year.
- Refer I-PL11 Vulnerability Management Policy.

External VAPT

- Internal VAPT shall be conducted to uncover any technical vulnerabilities of information systems.
- A qualified third-party service provider shall be engaged in conducting external VAPT.
- There shall be one external VAPT cycles per year.

Non-functional Developer Testing

- Non-functional developer testing should cover both information security and privacy aspects.
- Non-functional developer testing shall be carried out for customer projects by the development teams in their development environments.
- Non-functional developer testing shall be carried out before the product under test is deployed on to the QA environment.

Non-functional QA Testing

- Non-functional QA testing should cover both information security and privacy aspects.
- Non-functional QA testing shall be carried out for the
  - customer projects by the QA teams in their test environments.
  - changes to 99x information systems by the IT team in their test environment.
- Non-functional QA testing shall be carried out before the product under test is deployed on to the Production environment.

Non-functional production testing

- Non-functional production testing should cover both information security and privacy aspects.
- Non-functional production testing shall be carried out for the
  - customer projects by the QA teams in their production environments.
  - changes to 99x information systems by the IT team in the production environment.
- Non-functional production testing shall be carried out to
  - resolve related issues reported on the production environment.
  - verify the software products to be purchased by before the product under test is deployed on to the Production environment.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR12 Internal Audit & Review Process

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

L-PL01 Integrated Management System Policy

1. Purpose

Objective of this policy is to make sure that the organization consistently provides products & services that meet customer, organizational, legal and ISO standard requirements. It aims to enhance customer satisfaction through effective establishment, implementation, monitoring and improving of its processes.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy applies to operations of the entire company.

3. Policy Statements

- Basis of the Integrated Management System (**IMS**) shall be following standards/best practices.
  - Agile
  - ISO 9001:2015 - Quality Management System (**QMS**) requirements.
  - ISO 27001:2013 - Information Security Management System (**ISMS**) requirements and controls.
  - ISO 27701: 2019 - Privacy Information Management System (**PIMS**) requirements and controls as an extension to **ISMS**

Scope

- Scope of the **IMS** shall be identified considering.
  - Context of the business in terms of internal and external issues.
  - Understanding the interested parties of the business.
  - Understanding the requirements of the interested parties.
- Any exclusions from the scope of the **IMS** shall be clearly identified with a justification.
- Scoped **IMS** shall be
  - Established.
  - Implemented.

- Monitored.
- Continually Improved.

Establishing IMS

- Business strategy shall be established and reviewed annually to derive corporate objectives.
- Corporate objectives shall be planned according to the following department structure overlooked by the company leadership (Management and Corporate Leadership Team).
  - Business Development (BD)
  - Delivery (D)
  - Product (P)
  - HEX (H)
  - Technology (T)
  - Quality Engineering (QE)
  - Research (R)
  - People (P)
  - Marketing (M)
  - Finance (FI)
  - IT (I)
  - Facility (F)
  - Legal & Governance (L)
- Functions of all departments shall be recorded and maintained with an identification of criticality to business.
- Policies, Procedures and Work Instructions needed to support the **IMS** shall be identified with their interactions.
  - Policies - Intent of the management.
  - Procedures - Series of steps on how to achieve a policy.
  - Work Instructions - Additional optional details of a certain step of a procedure.

Implementing IMS

- Established **IMS** shall be implemented across the organization via different departments.

Monitoring IMS

- Implemented **IMS** shall be monitored for correct operations using following main activities.
  - Measurement & Analysis. - As an ongoing activity using defined metrices of relevant processes.

- Internal Audits and Product Health Reviews (**PHR**). Refer L-PL15 Information Systems Audit Policy
- External Audits - As a bi-annual activity with a third-party service provider
- Management Review on IMS - As a bi-annual activity with the company leadership.
- Internal Review on IMS- As an annual activity by the Compliance Manager.
- Management Meeting - As a weekly meeting.
- Corporate Leadership Meeting - As a weekly meeting.
- Support Management Meeting - As a bi-weekly meeting.

Continually Improving IMS

- Process improvements/changes shall be carried out as and when required.
- Following shall be considered as the main sources of process improvements.
  - Findings from external and internal audits
  - Improvements from **PHR** reviews.
  - Customer feedback
  - Employee feedback
  - Incidents
  - Management Review feedback
- Process improvements shall be recorded and followed up for completion with the focus of eliminating the root causes whenever possible.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR01 Integrated Management System Process

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

L-PL02 Quality Policy

1. Purpose

The purpose of this policy is to set the overall direction in terms of managing quality within the company operations.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees
☐ Permanent employees

- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- This is the top most policy for quality and it applies to all operations within the company.

3. Policy Statements

- Conform to ISO 9001:2015 Quality Management System requirements and agile principles.
- Build market winning products.
- Exceed customer expectations.
- Enhance Staff Competencies and Passion for Quality.
- Comply with applicable legal, regulatory, and contractual requirements.
- Continually improve the Quality Management System.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- All Processes.

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL03 Information Security Policy

1. Purpose

Purpose of this policy is to

- create an overall approach to information security
- detect and preempt information security breaches
- maintain the reputation of the organization

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- This is the topmost policy for information security, and it is applicable to all operations within the company.

3. Policy Statements

- Conform to ISO 27001:2013 Information Security Management System requirements while preserving the 99x culture and values.
- Ensure confidentiality of information.
- Ensure integrity of information.
- Ensure availability of information with minimal disruption to staff and customers as required by the business.
- Be accountable for the protection of personal data.
- Protect information assets from digital attacks.
- Comply with applicable legal, regulatory, and contractual requirements.
- Continually improve the Information Security Management System

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- All processes.

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL04 Privacy Policy

1. Purpose

Purpose of this policy is to ensure that the privacy of the individuals are protected and the personal data of individuals are processed according to the relevant regulations.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐

Permanent employees

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- This is the top most policy for privacy management and it applies to all operations within the company.

3. Policy Statements

- Conform to ISO 27701:2019 Privacy Information Management System requirements.
- Process personal data lawfully, fairly and transparently.
- Process personal data only for the purposes for which it was collected.
- Process personal data only for the relevant purposes for which it was collected.
- Keep personal data accurate and where necessary up to date.
- Do not keep personal data for longer than necessary.
- Process personal data in accordance with the privacy rights of the individuals.
- Comply with applicable legal, regulatory, and contractual requirements.
- Continually improve the Privacy Information Management System.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- All Processes.

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL05 Acceptable Use Policy

1. Purpose

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to 99x's established culture of openness, trust and integrity. 99x is committed to protecting its customers, employees, partners, data subjects and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy outlines the acceptable use of information and information processing facilities at 99x including but not limited to computer equipment, storage media, software systems, electronic mail, WWW browsing.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy applies to all information and information processing facilities, owned or leased by 99x.

3. Policy Statements

1. Intellectual property (IP)

- The software product you work on belongs to the customer. The product idea/concept, design, source code, etc are strictly the Intellectual Property (IP) of the customer.
- All other 99x data or intellectual property developed or gained during the period of employment remains the property of 99x.
- Employees who work with intellectual properties shall adhere to the relevant guidelines stated in the L-PL12 Information Classification Policy

Individuals must not

- act in a way the intellectual property is copied, leaked or made vulnerable for IP theft. Involvement in IP theft directly or indirectly is a punishable offence.
- retain such IP beyond termination or reuse for any other purpose.
- download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list).

2. Personally identifiable information (PII)

- Employees who process personal information must understand the requirements given in L-PL04 Privacy Policy.
- Employees who process personal information must also adhere to the relevant guidelines stated in the L-PL12 Information Classification Policy

Individuals must not

- process another persons personal information without consent.
- misuse personal information.

3. Processing information (other than IP or PII)

- When processing information, users must use appropriate security controls according to the classification level given in L-PL12 Information Classification Policy
- While 99x desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of 99x. As the management's concern is in securing company information, the safety of private information stored on company equipment or storage locations cannot be guaranteed.
- Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only 99x authorized mobile storage devices with encryption enabled must be used, when transferring confidential data.

Individuals must not

- process information classified as **Sensitive** or **Confidential** without the authorization from the management.
- disclose information classified as **Sensitive**, **Confidential**, **Restricted** or **Internal** without prior approval form the information owner.

4. Credential management

- All credentials are to be treated as sensitive, confidential information.

Individuals must not

- save credentials on paper or electronic medium.
- save credentials to have automatic log-on to systems. eg: Browser based systems

5. Remote working

- Information should be protected against loss or compromise when working remotely. Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- Laptops must be carried as hand luggage when travelling.

Individuals must not

- leave IT equipment unattended in public places.
- let family members, relatives and friends access company provided IT equipment.

6. Company property

- It is the responsibility of the employee to safeguard any property assigned to them both within and off office premises.
- In case of a loss / not finding the item at his / her work desk; it must be brought to the notice of the relevant department within 1 hours of observing the loss.
- All company property assigned to the employee, for example laptops, monitors, headsets & accessories, mobile devices including telephones, smartphones, USB memory devices, and access cards must be returned at termination of employment.

Individuals must not

- leave company property unattended.

7. IT equipment

- IT equipment provided by the company shall be used for the business purposed only.
- If unattended IT equipment is found within the office premises, it shall be handed over to the reception.

Individuals must not

- use the IT equipment provided by the company for personal work including but not limited to storing personal work (documents, music, videos, photographs, etc.)
- dismantle or physically tamper with computers or any other equipment without prior approval.
- leave the computers unlocked when the user is not around.
- leave equipment such as laptops, mobile phones, etc. unattended.
- use the laptop to store or transmit elicit material.
- use the laptop to harass others.
- hack into 99x system or any other system.

8. Mobile Phones

- Employees must use password protected smart phones to access corporate systems (email, MS Teams, Confluence, etc).

9. Social media presence

- Limited use of Company's infrastructure to engage in blogging and social media activities is acceptable, provided that it
  - is undertaken in a professional and responsible manner
  - complies with the Company's Social Media Policy
  - is not detrimental to Company's interests, and
  - does not interfere with an individual's regular work duties.
- Blogging from Company's infrastructure may be subjected to monitoring.

Individuals must not

- reveal any Company sensitive, confidential or proprietary information, trade secrets or any other material covered by Company's L-PL12 Information Classification Policy when blogging and posting on social media networks.
- engage in any blogging or social media activities that may harm or tarnish the image, reputation and/or goodwill of Company and/or any of its employees.
- make any discriminatory, defamatory or harassing comments when blogging, posting on social media networks or otherwise engaging in any conduct prohibited by Company's P-PL10 Anti-harassment Policy and P-PL11 Anti-discrimination Policy.
- attribute personal statements, opinions or beliefs to Company, or using Company's trademarks, logos or any other Company intellectual property without specific authorization from the management.

10. E-mail and Internet

- Use of internet and email is intended for business purposes only. Internet use for research and work-related learning is encouraged, however recreational and non-work-related activities should be minimized at office hours.
- All individuals are accountable for their actions on the internet and email systems.

Individuals must not

- use the internet or email for the purposes of harassment or abuse. Refer P-PL10 Anti-harassment Policy and P-PL11 Anti-discrimination Policy.
- use the internet or email to make personal gains or conduct a personal business.
- use the internet or email to gamble.
- place any information on the internet that relates to 99x, alter any information about it, or express any opinion about 99x, unless they are specifically authorized to do this.
- send unprotected sensitive or confidential information violating the L-PL12 Information Classification Policy.
- forward 99x emails to personal (non-99x) email accounts (for example a personal Gmail account).
- use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- open e-mail attachments received from unknown senders. (Which may contain viruses, e-mail bombs, or Trojan horse code).
- attempt to access blacklisted web site and application categories such as computer games, pornography, torrents, etc. using company resources (internet/devices). Refer 99x Blacklisted|Unauthorized Website and Application Categories

11. Software systems

- Users must use only licensed software and those must be used in accordance with the software supplier's license agreement.
- Users must keep all relevant software systems up-to-date as instructed by the IT team.

Individuals must not

- use blacklisted software. Please refer the list 99x Blacklisted|Unauthorized Website and Application Categories
- install 99x licensed software on computers not belonging to the organization.
- download any software from the internet without prior approval of the IT Department.
- copy any software owned by 99x.

12. Access control

- Access to the 99x systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the 99x systems.

Individuals must not

- allow anyone else to use their user ID/token and password on any 99x system.
- leave their user accounts logged in on an unattended and unlocked computers.

- use someone else's user ID and password to access 99x systems.
- leave their password unprotected (for example writing it down).
- perform any unauthorized changes to 99x IT systems.
- attempt to access data that they are not authorized to use or access.
- connect any unauthorized device to the 99x network or systems.
- store 99x data on any unauthorized IT equipment.

13. Anti-malware

- The IT department has implemented centralized, automated virus detection and virus software updates within the 99x. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not

- disable or uninstall the antivirus application already installed in the personal computers by the IT team.
- do not install additional antivirus software unless specific authority is obtained from the IT team.
- introduce malicious software ("Malware") onto the company network or performing other actions that might resulted in introducing such software.

14. Clear & Clean work areas

- The work area shall be kept clean.
- The rest room facilities shall be kept clean and dry.
- Sensitive or confidential information, specially on paper should be kept in locked drawers.
- All business-related printed matter must be disposed of using shredders.

Individuals must not

- leave sensitive or confidential material on printers, photocopiers or desktops.
- leave any information on white boards in meeting areas after the meeting/discussion is over.
- consume liquid food near IT equipment.

15. Source Code Management

- All source code should be maintained in designated repositories specified for the project.

- Employees should adhere to the practice of checking-in all code before they leave work each day.

16. Physical security

- Only the authorized personnel will have access to the office premises. All users who want to access office premises should follow the instructions given by the physical security personnel deployed in relevant locations.
- Employees shall notify the receptionist regarding their personal visitors prior to their arrival at the office premises.

Individuals must not

- make attempts to access the server room unless they are authorized to do so by the management.
- enter the office premises and/or perform duties under the influence of alcohol or similar narcotics.
- not allow their visitors into the restricted areas.

17. Utility services in office premises

- Employees must use water sparingly at office premises.
- Switch off lights, fans and Air-conditioning units not being used.

18. Personal belongings

- Safe custody of personal belongings brought into the office premises is entirely the responsibility of the particular employee.

19. Legal compliance

- Ensure compliance with all applicable laws and regulations.

20. Requesting support

- All IT support requests should be sent via email using itsupport@99x.io
- All Facility management support requests should be sent via email using adminsupport@99x.io.
- All HR support requests should be sent via email using hrsupport@99x.io.

21. Reporting breaches

- It is your responsibility to report suspected breaches of security policies without delay to the information security department.
- All information security and privacy breaches shall be reported by sending an email to SecurityIncidents@99x.io

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable

6. Classification

.

☐
Sensitive
☐
Confidential
☐
Restricted
☑
Internal
☐
Public

L-PL06 Corporate Compliance Policy

1. Purpose

The purpose of this policy is to

- promote 99x's commitment to compliance.
- facilitate good governance through a proactive approach to compliance management.
- promote a culture that values compliance.

2. Scope

2.1 Employment type

This policy is applicable to

☑
All employees
☐
Permanent employees
☐
Probation employees
☐
Contractual employees

Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- The Board and the management of 99x are committed to ensuring that the organization meets its Compliance Obligations.
- 99x is committed to meet the,
  - Contractual
  - Legal
  - Business (Policy) and
  - Standard, compliance requirements.
- Compliance requirements shall be clearly identified and assigned to the responsible parties within the company for implementation.
- Breaches of compliance requirements shall be reported as incidents and follow through as per the L-PL14 Incident Management Policy .

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be listed.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL07 Contract Management Policy

1. Purpose

The purpose of this policy is to provide a clear and standardized approach to managing and administering contracts between 99x and any third party (customers, employees, suppliers, etc.).

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐

Permanent employees

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- 99x approved standard contract templates are preferred wherever possible. Contract managers should consult legal services function if a contractor is not accepting the 99x standard contract templates.
- Employees shall never enter into verbal contracts on behalf of 99x.
- All contracts shall be signed by the authorized signatory for 99x.
- Contract management life cycle shall have following stages in it.
  - Contract Commencement - starts before a contract is signed.
  - Contract Management - runs until formal closure.
  - Contract Closure - the formal conclusion.
- Supplier Contract types:
  - Purchase orders - POs are a standard form of contract that is used for the purchase of simple, low risk items. PO should have the standard terms and conditions printed on it. If not, a copy shall be attached to it. Many suppliers provide their own terms and conditions when submitting a quote. These need to be carefully reviewed, as acceptance of the quote will result in acceptance of the supplier’s terms and conditions.
  - Standard Contracts - 99x has a number of standard contract templates to use for the provision of goods and/or services when a PO will not suffice
- All Contracts must include appropriate clauses in the areas of:
  - Work Health & Safety;
  - Quality Assurance;
  - Environmental;
  - Financial Capability;
  - Insurance;
  - Industrial Relations;
  - Performance;
  - Code of Conduct;

- Privacy Regulations (GDPR, SL PDPA, etc.)
- All Contracts must include appropriate Commercial clauses in the areas of:
- Payments and Retentions (or security);
- Price Adjustments;
- Delay to Completion (or delivery); and
- Processes to Resolve Claims and Disputes.
- Contract performance of all contracts must be regularly monitored, evaluated and reported.
- Contract Management begins with the awarding of a contract and should continue throughout the life of a contract until all the obligations under the contract have been satisfactorily completed, final payment has been made, and warranties have expired.
- Scope Management - The scope of each contract must be appropriately managed to ensure that all deliverables are properly received, payments are appropriately made, all timelines are met, and any extension options are appropriately exercised.
- Contract Amendments and Scope Changes - Contract extensions and amendments must not be used to expand a contract beyond what was agreed upon under the terms of the contract and the original procurement process, or to circumvent the need to procure additional deliverables through a competitive process. During the course of a contract, additional work may arise that could not be anticipated during the project planning process. Contract amendments for adjustments to the scope of the contract may be approved if the adjustment is for work that is directly connected or incidental to the original contract scope. Supplier Management Policy Page 2 of 13 If a contract amendment results in a net increase to the contract value previously approved, the amendment must be approved in accordance with the County's Schedule of Approval Authority. All amendments to an existing contract must be appropriately documented. Legal Services could be consulted regarding all matters pertaining to contract interpretation and application, and for any changes, extensions, renewals, or amendments required to be made to any executed contract.
- Contract Disputes - All potential contract disputes with suppliers must be managed in accordance with the dispute resolution mechanisms outlined in the contract. Where a contract is silent on dispute resolution, Departments must ensure that potential disputes are proactively managed and appropriately escalated. Written copies of all communications and correspondence with suppliers concerning a contract dispute must be maintained by the Department.
- Early Termination - A contract can only be terminated prior to its expiry date with the involvement of Legal Services and/or the CEO and in accordance with the terms and conditions outlined in the contract.
- Risk of Legal Action - Legal Services and/or the CEO must be promptly advised if a supplier initiates or threatens legal action against the County at any time throughout the

life of the contract or if there are signs that a supplier is experiencing financial difficulty (e.g. the supplier fails to pay its employees, suppliers or subcontractors).

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be listed.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL08 Change Mangement Policy - DRAFT

1. Purpose

The purpose of this policy is to manage changes in a well-communicated, planned and predictable manner that minimizes unplanned outages and unforeseen system issues. Effective change management requires planning, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the users.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

-

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

-

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☐ Internal

☐ Public

L-PL09 Knowledge Management Policy

1. Purpose

2. Scope

2.1 Employment type

This policy is applicable to

- [ ] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

-

3. Policy Statements

-

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

-

6. Classification

.

- [ ] Sensitive
- [ ] Confidential
- [ ] Restricted
- [ ] Internal
- [ ] Public

L-PL10 Non-Conformance Management Policy

1. Purpose

2. Scope

2.1 Employment type

This policy is applicable to

- [ ] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

3. Policy Statements

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

-

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☐ Internal

☐ Public

L-PL11 Document Management Policy

1. Purpose

Purpose of this policy is to set guidelines in maintaining and controlling information that is deemed required by the organization.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Applicable to documents of all form (physical or digital).

3. Policy Statements

- Documents (also referred as documented information or information in relevant context) based on following requirements shall be maintained.
  - Requirements of ISO 9001, 27001 and 27701 standards.
  - Policies, Procedures and Work Instructions as required by the company.
  - Operations as required by the relevant project or department.

Creation and Update

- When a document is created, it should have appropriate
  - Title.
  - Date of creation.
  - Author.

Document	Created by	Updated by	Reviewed by	Approved by
Policies	Management Team	Management Team	Management Team	Management Team
Procedures & Work Instructions	Department/ Project Team	Department/ Project Team	Management Team	Department Head / Tea Lead
Operational documents	Department/ Project Team	Department/ Project Team	Department Head / Team Lead as required	Department Head / Tea Lead as required

- Documents shall be reviewed for suitability & adequacy and kept up to date where necessary.

Control of Documents

- Documents shall be appropriately access controlled.

Document	Viewed By
Policies	All employees / External parties depending on the policy
Procedures & Work Instructions	All employees / External parties depending on the process
Operational Documents	Management Team / Department Team / Project Team

- Revision history of documents shall be maintained to identify the:
  - Incremental revision number
  - Change
  - Date the change was made
  - Person who made the change
- Previous revisions of a document shall be available for use if required.
- All hard copies shall be put inside files with clear labels. Files shall be kept with a suitable means of storage.
- Retention period of all documents shall be decided as given below. At the end of the retention period, those shall be archived or disposed.

Document	Retention
Policies	As long as required by the organization.
Procedures & Work Instructions	As long as required by the organization.
Operational – non personal information	As long as required by the organization.
Operational – personal information	L-PL19 Personal Data Disposal Policy

- Obsolete documented information shall be clearly identifiable if they are retained for any purpose.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

L-PL12 Information Classification Policy

1. Purpose

The purpose of this policy is to establish a framework for classifying information based on its sensitivity, value and criticality to the organization, so that the corporate and customer information can be secured appropriately.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy covers information assets of below types **at rest** and **in transit**.
  - Email
  - Digital (eg: MS word, MS Excel, Powerpoint, Source code, etc.)
  - Systems (eg: information in HCM, Maturify, Confluence, Social media platforms, etc.)
  - Paper
  - Communication channels (eg: Skype, Slack, MS Teams, Facebook, White boards, etc.)
  - Verbal
- Following special roles are applicable for this policy.
  - Information owner (The person who is ultimately responsible for the information being collected and maintained by his or her department or division).
  - Information custodian (Engineers from the IT department or, the Information Security office. Custodians are responsible for maintaining and backing up the systems, databases and servers that store the organization's data. In addition, this role is responsible for the technical deployment of all of the rules set forth by information owners and for ensuring that the rules applied within systems are working.).
  - Information users (Person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the information owner. Information users must use information in a manner consistent with the purpose intended, and comply with this policy and procedures).

3. Policy Statements

- All information assets to be classified using below Information Classification Levels.

- **Public** - Information that is already available to public without restrictions. Examples include
  - Content published on company web site, company Facebook and other similar social media profiles.
  - Content on company brochures and banners used in external events.
  - Content presented about company on public events.
  - Press releases.
- **Internal** - Information that may be proprietary in nature, and is not intended for external viewing or consumption. Available to any member of staff. Typically, if this level of information leaked outside of the organization, it could be **inappropriate**. Examples include
  - Maturify models open for all staff.
  - Policy and Procedure documents open for all staff.
  - Internal emails and memos.
  - Business strategy presented to entire staff.
- **Restricted** - Information that may be proprietary in nature, and is not intended for external viewing or consumption. Available only to specified members of staff with appropriate authorization. A breach could results in a **considerable damage** to the company. Examples include
  - Company resource plan.
  - Department risks.
- **Confidential** - Information that is considered confidential. Available only to specified members of staff with appropriate authorization. A breach could results in a **serious damage with lasting negative consequences** to the company. Examples include
  - Company Financial Information
  - Employee salary information
  - Passwords
  - Credit Card Information
  - Bank account details
- **Sensitive** - Information that is considered highly sensitive, may be subject to regulatory oversight. Available only to specified members of staff with appropriate authorization. A breach could result in a **litigation with lasting negative consequences** to the company. Examples include
  - **Sensitive - PII**
    - PII under GDPR, SL PDPA and other similar regulations
  - **Sensitive - IP**
    - Customer IP including source code and product ideas.
    - Customer product specifications, backlog items, system documentation, etc.

- Any information which is not explicitly classified will be classified as Confidential - Pending Classification, by default to avoid data leakage. Rules applicable for the level of Confidential information will be applicable in such instances.
- If the same asset contains more than one type of information, then the asset takes the classification which requires the highest protection. eg: An employment letter has personal information (Classification = Sensitive) and salary information (Classification = Confidential) hence it should be classified as Sensitive.
- Where a third party will be responsible for handling the information on behalf of the com pany, the third party shall be required by contract to adhere to this policy prior to the sh aring of information.
- Any asset which is not considered as an information asset will also need to be classified in compliance with above classification levels based on the type of information they hold. Eg: a laptop which has no data will not be classified but once it has confidential information it will be classified as a "Confidential" asset.
- Where information is discovered to have been incorrectly classified, or not to have been managed in accordance with its Information Classification, this should be reported imme diately to the information security incident help desk by sending an email to SecurityIncidents@99x.lk

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR02 Information Classification Process

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☐ Internal
☑ Public

L-PL13 Information Transfer Policy

1. Purpose

To control the flow of information in a secure manner between the organization and internal/external entities.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees
☐ Permanent employees
☐ Probation employees
☐

Contractual employees

Internship employees

2.2 Other scope elements.

- This policy is applicable to all third parties who work with 99x.
- This policy is applicable to information in any form (digital, physical, verbal, etc.) of any classification level.
- This policy covers transfer of information
  - within the organization.
  - from third parties to the organization.
  - from organization to third parties.

3. Policy Statements

- Understand the classification of information being transferred. Refer L-PL12 Information Classification Policy and the rules defined under its process L-PR02 Information Classification Process.
- Transferred information shall be protected from interception, copying, modification misrouting and destruction.
- It is dangerous to assume that because someone asks for information that they are necessarily authorized
  or legally entitled to receive it. Verify this and get explicit authorization from the information owner for the transfer. For **Sensitive-PII** information (personally identifiable information/personal data), the owner is the Data Subject.
- It is the information sender's responsibility to ensure that the transfer is
  - Legal and necessary.
  - free of any associated risks.
- The external party must acknowledge receipt of the information transferred.

Agreements on Information Transfer

- Personal Data Transfer Agreements with Customers -
  - if **Sensitive-PII** information (personally identifiable information/personal data) is transferred from customer to 99x, then the data transfer agreements shall be signed. According to the Schrems II verdict, data transfer to third countries with no adequacy decision shall accompany a Data Transfer Impact Assessment (DTIA) on the legal risks under GDPR. However Digital Nomads type remote employees are not considered a "data transfer" under GDPR hence does not require the DTIA.
- Personal Data Transfer Agreements with Suppliers

- if **Sensitive-PII** information (personally identifiable information/personal data) is transferred to suppliers from 99x to a different jurisdiction, then the parties shall enter into a data transfer agreement according to the applicable privacy laws of 99x legal entity.

Non-Disclosure Agreements

- Confidentiality or Non-Disclosure Agreements shall be signed for **Confidential**, **Sensitive-IP** or **Sensitive-PII** information transferred to third parties. These agreements shall be signed by authorized signatories from both parties. Following entities shall have NDAs with 99x accordingly.
  - Employees.
  - Customers.
  - Suppliers.
  - Partners.
- When an agreement is terminated, all information shared with the other party in the form of
  - Hard copies shall be taken back and shredded.
  - Softcopies shall be taken back.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR09 Information Transfer Process

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☐ Internal
☑ Public

L-PL14 Incident Management Policy

1. Purpose

Purpose of this policy is to set guidelines in reporting and responding to information security and privacy incidents in a quick, effective and orderly manner to minimize negative effects.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees
☐ Permanent employees

- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- An information security or privacy event, weakness or incident (Commonly referred as **Incidents** here after in this policy) is an action which might put
  - the Confidentiality of an information or information processing facility directly or indirectly at risk.
  - the Integrity of an information or information processing facility directly or indirectly at risk.
  - the Availability of an information or information processing facility directly or indirectly at risk

Reporting

- All incidents shall be reported immediately to SecurityIncidents@99x.io.
- Employees shall make no attempts to prove an incident.
- CISO or DPO shall be contacted for further information.

Assessment

- Reported incidents shall be assessed by the CISO to decide the further actions. DPO shall be consulted in assessing privacy incidents.

Response

- Incident response team shall be identified with their responsibilities in responding to an incident.
- The aftermath of an incident shall be handled in a way that limits damage and minimize recovery time and cost.
- Corrective action identified shall be implemented without undue delay to limit the frequency, damage and cost of future occurrences.

- Relevant evidence shall be collected and preserved with relate to an incident, irrespective of the necessity of legal actions.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR07 Incident Management Process

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL15 Information Systems Audit Policy

1. Purpose

Regular audits help to ensure that controls are sufficient and effective at providing information confidentiality, protecting Personally Identifiable Information (PII), ensuring system availability, and fostering a higher degree of data integrity. This policy sets forth 99x's practice regarding information system related audits.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy covers all information systems of 99x including software and hardware systems.
- This policy covers all organizational functions except Finance.

3. Policy Statements

- Following information system audits are applicable.

- Internal audits.
- External audits.
- Third-party audits.
- Internal VAPT
- External VAPT
- Non-functional developer testing.
- Non-functional QA testing.
- Non-functional production testing.

- These audits shall be conducted as planned activities according to a schedule.
- Audit findings shall be recorded and assigned back to the relevant auditee. Follow up audits shall be conducted to verify the implementation of the findings.

Internal Audits

- Internal Audits shall be conducted to verify the conformity to all compliance requirements of,
  - Departments.
  - Customer Projects. Internal audits conducted on customer projects are called Product Health Reviews.
- Internal audits shall be conducted by 99x employees who are trained on conducting such audits.
- Internal Audits shall be independent and shall not cover the own implementations of the auditor.
- There shall be two internal audit cycles per year.
- When conducting the audits, the internal auditors will get access only up to the level they have clearance for access.

External Audits

- External audits shall be conducted to verify the conformity to the relevant ISO standard requirements as specified in the L-PL01 Integrated Management System Policy.
- A qualified third-party service provider shall be engaged in conducting external audits.
- There shall be two external audit cycles per year.
- When conducting audits, the external auditors will get access to any information required.

Third-Party Audits

- Third-party audits shall be conducted on selected suppliers to verify the conformity of their internal processes to relevant ISO standards.
- A qualified third-party service provider shall be engaged in conducting third-party audits.

- Third-party audits shall be conducted as and when they are required.

Internal VAPT

- Internal VAPT shall be conducted to uncover any technical vulnerabilities of information systems.
- Internal VAPT shall be conducted by 99x employees who are trained on conducting such audits.
- There shall be two internal VAPT cycles per year.
- Refer I-PL11 Vulnerability Management Policy.

External VAPT

- Internal VAPT shall be conducted to uncover any technical vulnerabilities of information systems.
- A qualified third-party service provider shall be engaged in conducting external VAPT.
- There shall be one external VAPT cycles per year.

Non-functional Developer Testing

- Non-functional developer testing should cover both information security and privacy aspects.
- Non-functional developer testing shall be carried out for customer projects by the development teams in their development environments.
- Non-functional developer testing shall be carried out before the product under test is deployed on to the QA environment.

Non-functional QA Testing

- Non-functional QA testing should cover both information security and privacy aspects.
- Non-functional QA testing shall be carried out for the
  - customer projects by the QA teams in their test environments.
  - changes to 99x information systems by the IT team in their test environment.
- Non-functional QA testing shall be carried out before the product under test is deployed on to the Production environment.

Non-functional production testing

- Non-functional production testing should cover both information security and privacy aspects.
- Non-functional production testing shall be carried out for the

- customer projects by the QA teams in their production environments.
- changes to 99x information systems by the IT team in the production environment.
- Non-functional production testing shall be carried out to
- resolve related issues reported on the production environment.
- verify the software products to be purchased by before the product under test is deployed on to the Production environment.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR12 Internal Audit & Review Process

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL16 Procurement Policy

1. Purpose

Purpose of this policy is to set guidelines to ensure that 99x gets the highest quality of desired products and services at the best price possible while adhering to the procurement principles.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy is applicable to products and services.

3. Policy Statements

Procurement Principles

- All procurement activities must be undertaken in accordance with the following core principles.
  - Value for money - strive to obtain the maximum value for the money spent.
  - Probity and equity - including open and effective competition, fairness and impartiality, transparency, security and confidentiality.
  - Conflict of Interest - ensuring appropriate oversight to ensure that probity and equity principles are adhered to and that no conflict of interest would exist when an employee, his/her family member, business partner or organization has a financial or other interest and/or gain in the vendor selected.
  - Gifts and Hospitality - where the 99x staff member receives gifts or any other benefits from current or prospective Suppliers, the L-PL18 Gift Acceptance Policy must be applied.
  - Social Sesponsibility – subject to costs and other considerations, use best efforts to purchase products and/or services that are socially and environmentally friendly and sustainable, including consideration of the disposal of such goods.

Identifying the Need for Procurement

- First, the need for a product or service must be identified. This could turn out in one of two ways.
  - Identifying the need to buy a new product or service.
  - Reordering a product or service when existing stock or output falls below a certain threshold.
- Key stakeholders must be consulted before deciding the need for a product or service.
- Criticality of the need must be identified based on the department function to which the need is related to.

Procurement Planning

- Procurement planning must be part of the annual budgeting process. (Refer FI-PL01 Budget Policy)
- Department Managers are responsible for planning his/her department's estimated procurement needs on an annual basis.

Sourcing Suppliers

- Research must be conducted to look for suppliers that can provide the required product or service.
  - Trade Publications - Typically magazines and online websites, these publications are industry-specific and oftentimes feature relevant and trustworthy suppliers.

- Trade Associations - Also referred to as industry trade groups, trade associations are organizations created for specific professions. If requested, members will offer supplier recommendations.
- Professional Recommendations - Business associates, colleagues, and experienced executives can give insight into suppliers they have worked with.
- Directories - Local suppliers can be found in various business directories.
- Trade Shows - These events enable business owners to meet and interview relevant suppliers in person.

- For new purchases, the process of identifying and vetting potential suppliers to determine their quality, pricing, reliability, etc. shall be followed. For repeat orders, the team can simply choose from a list of existing suppliers.
- The team involved shall request and compare quotes from different suppliers before making a final purchase decision.

Selecting Suppliers

- Careful selection of suppliers should be done to ensure that best possible price, quality and delivery time available within the markets is obtained.
- A list of suitable suppliers (the list of pre-qualified suppliers), for each type of goods and services based on past performance shall be maintained. Refer L-PL17 Supplier Management Policy.
- Following selection criteria-based scoring mechanism must be used in selecting a supplier.
  - Suitability of Product/Service.
  - Price.
  - Discounts.
  - Delivery.
  - Financial Strength.
  - References.
  - Customer Service.
  - Compliance (Information Security, Privacy and Legal).
  - Integrity.
  - Terms and Conditions.
  - ESG Sustainability.
  - Response.
- Information pertaining to above selection criteria must be saved.
- Purchases exceeding 50,000/= LKR shall have at least two quotations from two suppliers.
- The team involved should negotiate the terms of the purchase with each vendor to get the best possible supply at the best value.

- Department Manager shall select the best supplier based on the above selection criteria and get the approval from the relevant member of the Management Team.
- Department Manager shall get the relevant supplier agreements signed by the authorized signatories of both 99x and supplier.

Purchasing

- The team involved shall raise purchase order and get it approved by the Chief Financial Officer if the amount is greater than the allowed petty cash amount.
- The approved purchase order shall be sent to the selected supplier.

Inspection of Received Products/Services

- The team involved shall inspect any supplied goods and services and ensuring that they match the specifications outlined in the purchase order.
- However, if the quality or condition of the supply deviates from the terms accepted by both parties, the supplier will have to retake the delivery until the problem is fixed.

Payment

- The team involved shall forward all documents relating to the order to the company's finance department for payments.
- Any discrepancies will have to be resolved before payment is approved. If there are no problems, the payment is made through the channels defined in the contract's terms and conditions.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be listed.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL17 Supplier Management Policy

1. Purpose

Purpose of this policy is to set guidelines for mitigating the risks associated with supplier's access to the organization's assets.

2. Scope

2.1 Employment type

This policy is applicable to

☑

All employees

Permanent employees

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- This Policy applies to any third party that provides goods or services to 99x.

3. Policy Statements

Onboarding and Managing Suppliers

- Suppliers approved for procuring products and services shall be recorded and managed centrally. Following information about suppliers shall be captured at a minimum.
  - Contact information.
  - Owner (99x department).
  - Criticality to business.
  - Type of Service/Product
  - Need for a contract.
  - Need for a Non-Disclosure / Confidentiality Agreement.
  - Information being shared including personal data.
  - Additional information security and privacy requirements.
  - Evaluation of performance.

Information Security Requirements

- The information security provisions in place at suppliers must be clearly understood and improved where necessary.
- The information security requirements and controls must be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract as appropriate. It should cover following points at a minimum,
  - requirements and obligations inherited by 99x in contracts with other parties (eg: customers).

- The classification of any information that is to be processed by the supplier.
- the need to obtain permission to share 99x information beyond the supplier.
- Minimum organizational and technical measures the supplier should implement (like ISO 27001 and ISO 27701) in order to meet 99x's PII protection obligations as per applicable privacy regulations (eg: EU GDPR).
- the need for security requirements to be cascaded consistently and where applicable to all sub-contractors of the primary supplier throughout the supply chain.
- the requirement for management and reporting of actual and suspected incidents.
- the need for performance monitoring and reporting in order to identify and remediate non-compliance, poor performance, ineffective technical controls, or incidents.
- the right to audit the supplier and their supply chain.
- an exit plan (which includes data migration) and the terms on which 99x has a right to terminate.

- Access to 99x information must be limited where possible and shall be according to a clear business need and as per the information security policy. Access shall be granted as per the requirements of https://seranet.atlassian.net/wiki/spaces/IT/pages/3728048259.
- The information security status of suppliers shall be assessed/validated depending on criticality and the volume of the information being shared with them. This could be,
- an internal audit conducted by the Compliance department of 99x, or
- a third-party audit conducted by an independent party on behalf of 99x.

Retiring Suppliers

- A method for exiting, terminating, renewing, and renegotiating contracts with suppliers shall be established. It should cover,
- establishing a method to determine whether to exit, terminate, renew, or renegotiate a contract.
- revocation of physical and logical access to 99x information.
- return, transfer, or verified secure destruction of assets.
- maintaining compliance with license agreements and intellectual property rights.
- follow up on termination activities.

Reviewing Suppliers

- Supplier records of the entire company shall be reviewed bi-annually by the Compliance department.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non-Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR17 Supplier Management Process

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL18 Gift Acceptance Policy

1. Purpose

Gifting is a widespread aspect as a customary practice. However, Gifts can be seen as bribes and they may be intended to influence decisions of an organization or create reciprocal obligations. While it is discouraged to accept or offer (directly or indirectly) gifts or entertainment from customers, suppliers, or any other business associates of the company, however in some situations it is considered customary to accept gifts.
This policy defines guidelines and acceptable norms for accepting of gifts.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- An employee should not accept any reward that is valued more than USD 500.
- An employee should not accept cash rewards.
- An employee may accept rewards of following form
  - A reward that can enhance an individual's career and his/her personal growth, for Eg. a sponsorship for a technological seminar or any other event that the individual is interested in and which will enhance his/her ability in the work.
  - A device which can be used as a personal device and can be used in project activities.

- The party who offers the gift should always keep 99x management informed before giving a reward to 99x employees. 99x reserves the right to agree or disagree in accepting the reward.
- It will be considered as a violation of the company code of conduct to ask for a reward from a third party or in anyway pressurize a third party into giving a reward by any of the 99x employees.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☐
Internal
☑
Public

L-PL19 Personal Data Disposal Policy

1. Purpose

To ensure that methods of personal data disposal meet the requirements of the EU GDPR and other applicable privacy regulations.

2. Scope

2.1 Employment type

This policy is applicable to

☑
All employees
☐
Permanent employees
☐
Probation employees
☐
Contractual employees
☐
Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- When the PII is no longer required for the identified purpose, all such data including those in backups and those transferred to third parties must be disposed of securely.
  - Physical documents - Minimum standard for disposal of paper based information would be shredding. This should not be delegated if the confidentiality of the operation cannot be ensured.
  - Electronic documents - These should be permanently deleted from all storage locations including backups.
  - Information systems - These should be permanently deleted from all storage locations including backups.
  - Emails - These should be permanently deleted from all storage locations including backups.
  - Communication channels -While it is discouraged sharing personal information via unsecured social media communication channels, if it is done for some reason then those should be permanently deleted from all storage locations including any backups of images, screen shots etc.
- Once deleted, the PII data shall not be retrievable.
- PII data deletion shall not be contracted to third parties.
- Permanent deletion of any PII transferred/disclosed to third parties shall also be ensured.
- PII deletion shall be done under the instruction of the Data Protection Officer.

Retention

- PII Retention periods are as given below.

Role of 99x	PII	Retention
PII Controller	Name, email address, designation of data subjects from EU/EEA and SL	As long as required by the organization
PII Processor/Sub Processor	Production grade PII - (for product testing)	Until the specific testing is
PII Processor/Sub Processor	Name, email address, designation of employees of customers	Until the business contract ends.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

L-PL20 Exceptions Policy

1. Purpose

The policy and associated guidance provide a well-defined approach to review exception requests for published 99x policies, processes and standards.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- 99x policies, processes and standards are developed based on business, regulatory and industry requirements. 99x recognizes objectives and technology needs for the departments may be impacted by compliance requirements.
- The employees who are not able to meet the policies, processes and standards will submit an exception request to the relevant department.
- Exception requests will be reviewed by a relevant member of the management team on a case- by-case basis to identify the risk for impact to the business, not every exception may be able to be approved and implemented.
- Exceptions are valid only up to a period of 12 months.
- Requests for an exception for convenience will not be approved.
- Until approval has been granted the requested exception will not be implemented.
- Exception status may change at any time due to an incident or significant risk to 99x information, network, or systems.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be approved by the management in advance.

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- L-PR20 Exceptions Process

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

L-PL21 Risk Management Policy

1. Purpose

2. Scope

2.1 Employment type

This policy is applicable to

- [ ] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

-

3. Policy Statements

-

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

-

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☐ Internal
☐ Public

FI-PL05 Salary Advance Policy

1. Purpose

A salary advance is given as an emergency short term loan where the employee may have an extraordinary need for personal reasons.

2. Scope

2.1 Employment type

This policy is applicable to

☐ All employees

☑ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- A salary advance refers to employees receiving a portion of their pay before their next normal payday.
- An employee could request a maximum of 03 salary advances per annum.
- The maximum amount of advance pay is 50% of the employee's basic salary.
- The salary advance needs to be settled in full from the next processed payroll.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- FI-PR01 Salary Advance Process

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

FI-PL02 Employee Bonus Policy

1. Purpose

This policy explains how 99x distributes bonuses to it’s employees.

2. Scope

2.1 Employment type

This policy is applicable to

☐ All employees

☑ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- An employee is eligible to receive the bonus upon completing 02 years in service as of 31st December of a given year.
  - ***Eg 1**. Employee **A** joins 99x on 1st December 2019 and completes 2 years on 01st December 2021. As **A** completes 2 years by the cutoff date December 2021, A will receive the 1st part of the bonus in December 2021.*
  - ***Eg 2**. Employee **B** joins 99x on 1st March 2020 and completes 2 years on 1st March 2022. As **B** completes 2 years by the cutoff date December 2022, B will receive the 1st part of the bonus in December 2022.*

3. Policy Statements

- The bonus scheme is based on a profit sharing model where 10% of the annual company profits is disbursed as bonus among the employees.
- An employee's bonus % will be made up of percentage components being added from each of the following dimensions.

Dimension	% added
Being identified as a key resource in the Company - identified by management team in the team - identified by the CL team ** as the key resource selection process is not prevalent at the moment, this component will be distributed among the other dimensions	40%
2. Number of years in the Company	ranges from 4 to 55%
3. Annual appraisal score	ranges from 3 to 75%

4. Special project bonus 25%-50%

Account managers of large teams are entitled to a special project bonus, based on team size and % of company revenue generated

team size > 10 team members
% of company revenue generated > 10%

Eg. *A has been at 99XT for 2 years. Got an appraisal score of 96% at the last appraisal*

His bonus percentage would be 100% of his basic salary (40+60)

- The bonus payment will be made based on the company performance for it's calendar year which is from January to December.
- The 1st part of the bonus will be paid in December and the 2nd part based on the company performance and above criteria will be paid in April of the following year.
- All %s are calculated against the basic salary.
- These %s are subject to change annually, based on company performance.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be defined.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

FI-PL03 Tax Payment on Employment Benefits Policy

1. Purpose

The purpose of publishing the tax payment policy on employment benefits is to educate our employees about the changes in the new Income Tax scheme, create awareness and emphasize that income tax filing will be the sole responsibility of the employee.

The policy will come into effect from 1st May 2020 and any changes and addendum to the policy will be notified via an email.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

- Permanent employees
- Probation employees
- Contractual employees
- Internship employees

2.2 Other scope elements.

- An employee is liable to pay income tax if his aggregated income from all sources fall in the below categories ,

Period	Income Range
Year of Assessment – 2019 / 2020	LKR 250,000 and above per month or
(January 2020 to March 2020)	LKR 750,000 and above per quarter
Year of Assessment – 2020 / 2021	LKR 250,000 and above per month or
(April 2020 to March 2021)	LKR 3,000,000 and above per annum

3. Policy Statements

- The company tax payment process is described below,

Period	Tax Scheme	Tax remittance to Dept of Inland Revenue (DIR)	Tax deduction from the employee
January 2020 to March 2020	PAYE scheme	The company will make the tax payment on behalf of the employee.	The tax payment will be recovered from the respective employees through the May 2020 salary payment.
April 2020	APIT Scheme	The company will make the tax payment on behalf of the employee.	The tax payment will be recovered from the respective employees through the June 2020 salary payment.

May 2020 onward	APIT Scheme	Company will remit the tax payment on or before 15th June 2020.	The tax deduction will be made through the respective month's payroll

Note. The tax deduction is remitted to the DIR on or before the 15th day of the following month commencing from May 2020.

- An APIT certificate with details of the tax deductions made during the year will be issued to employees before the expiry of the 30th day of April in the following year or where employment ceases during the year of assessment, not more than 30 days from the date of ceasing employment.
- In compliance to the scheme the company will furnish the annual statement, with the payment schedules of all employees to the commissioner general by 30th April every year.

Employee's obligations

- Employee's will need to furnish the employment declaration and hand it over to the accounts team (Moin / Revathy) on/before 5th of May.

APIT_001_EST.pdf
17 Sep 2022, 03:46 PM

- It is a responsibility of the employee to make the tax payment on his taxable income including the employment gains and profits, in the absence of the employment declaration form submission where the company will not deduct the tax
- Committed tax liabilities on behalf of the employees will be recovered from an employee's final settlement if an employee discontinues the employment through resignation, retirement, etc.
- The company has the right to request a tax clearance if an employee resigns without proper notice.
- The employee must file a tax return irrespective of the APIT deduction. The DIR has facilitated an online application process to obtain a Taxpayer Identification Number (TIN).

(Please follow the link for taxpayer registration) Access To e-Services

Applicable Tax rates

For Y/A 2019/20 Last Quarter (Jan 20 to March 20)

Cumulative Gains and Profits from the Employment (Rs.)	Tax Rate
0 -750,000	Nil
750,001- 1,500,000	6 %
1,500,001- 2,250,000	12 %
2,250,001 & above	18 %

For Y/A 2020/21 (April 20 to March 21)

APIT 2020-21.pdf
17 Sep 2022, 03:47 PM

Prepared on: 1st May 2020

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

FI-PL04 Expense Reimbursement Policy

1. Purpose

Purpose of this policy is to set guidelines to repay employees for any out-of-pocket expenses that they have incurred on behalf of 99x.

2. Scope

2.1 Employment type

This policy is applicable to

☐ All employees
☑ Permanent employees
☐

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- Employee has to complete one year of service.

3. Policy Statements

Travel

- fd

Food and beverages

- fds

Home internet connection

-

Professional Exams and Memberships

- Employees will be able to reimburse up to
  - 100% of the Course fees, Registration fees.
  - 100% of the Examination fees.
  - 100% of Membership fees to Professional bodies, under following conditions.
- Management approval must be taken before registering for any course or to a membership.
- The courses and the memberships should be related to the present position of the employee or for the potential development of the company.
- These reimbursements will depend on the allocation for the relevant budget for that year.
- Employees will need to serve a minimum of 1 Year for every reimbursement from the claim date or pay back the whole sum if resigned pre mutually.

Exams

- The course should be taken at the employees own time outside normal working hours.
- Reimbursement will be made only on satisfactory proof of successful completion of the examination at the first attempt and supported by receipt.
- Reimbursements will be made only for examinations conducted in Sri Lanka.
- Certifications taken should be at an accredited Institute recognized by the company.
- A list of approved certifications/Examinations is as follows.
  - Microsoft
  - Java
  - Oracle
  - CIMA Certification*
  - Project Management Professional (PMP)
  - CSTE (Certified Software Test Engineer) – QAI
  - CTFL (Certified Tester-Foundation Level) - ISTQB
- *CIMA Reimbursement is made available only to the BA team members. The Reimbursement includes only the Exam Fee and the Annual Subscription. The Reimbursement made is also limited to a Maximum of RS 43,000 annually. To be entitled for the CIMA Reimbursement the candidate should fulfill the requirements mentioned in the "CIMA reimbursement policy guide".

Memberships

- All leads and above are eligible to reimburse professional membership fee from one professional body listed below. This includes the annual renewing fee. Membership should be in relevance to the career.
  - IET (The Institution of Engineering and Technology)
  - IEEE
  - ACM (Association for Computing Machinery)
  - CSSL
  - AST (Association for Software Testing)
  - BCS
  - Scrum Alliance
  - IIBA**
  - PMI
  - ACCA, CA, CMA
  - ISACA
- **IIBA Annual Membership will be made available to team members who has perform duties of a project business analyst for two projects, or for more than a year or hold a designation equivalent to Business Analyst or above.

Other

- fdsfs

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be added

6. Classification

.

☐ Confidential

☐ Personally Identifiable Information

☐ Restricted

☑ Internal Use

☐ Public

P-PL01 Code of Ethics & Conduct Policy

1. Purpose

The Code of Ethics and Conduct describes the minimum standards of behavior required of all 99x employees. These standards are to serve as a guide when making decisions and taking actions.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- Our guiding principles are;
  - **Trust and Openness** - We are successful because employees trust the leadership and have an amazing relationship with all Xians. We do the right thing even when no one is watching.

- **Innovate by continuously learning** - We are current on market developments through continuous learning. This fuels our innovation which enables our clients to build impactful products.
- **Responsible work ethic** - We strive to safeguard the trust and confidence our clients place in us. We are disciplined, accountable, transparent and aim to do the right thing, always.
- **Courage to push boundaries** - We don't blindly follow instructions. We challenge ourselves to see how things can be done better and are brave enough to champion these ideas.
- **Freedom to lead** - We work in a company where everyone is a Leader. We are given the freedom to take ownership and lead in our field and are never restricted by a title.
- **Nurture your passion** - We pursue our passions to reach great heights in the local industry and globally. The company and fellow Xians invest, mentor and encourage this journey.
- **Deliver excellence** - We build impactful digital products by striving for excellence. We aim to exceed customer expectations by consistently delivering value with quality.
- **Diversity and inclusion** - We have an equal opportunity culture that genuinely welcomes and cares about each employee. Our caring culture overflows to touch the community around us.
- **Celebrate together** - We are quick to celebrate team accomplishments and any Xian's success. We are willing to learn and improve ourselves in case we fall short.

- We behave at all times in a manner consistent with the company's guiding principles.
- We support and encourage others to comply with the guiding principles.
- We comply with the governing laws of the land.
- We behave at all times in a manner that enhances the reputation of 99x.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL02 Attendance Policy

1. Purpose

The purpose of this policy is to set forth guidelines for handling employee absences and tardiness to promote the efficient operation of the company and minimize unscheduled absences.

2. Scope

2.1 Employment type

This policy is applicable to

- [x] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- This policy is applicable for both “working from office” and “remote work” models.
- This policy is not applicable for absences due to planned leave.

3. Policy Statements

- Punctual and regular attendance is an essential responsibility of each employee at 99x.
- Working hours are from 8.00 a.m. to 5.00 p.m. or 9.00 a.m. to 6.00 p.m..
- Employees are expected to report to work as scheduled, on time and prepared to start working.
- All employees should record in and out times.
- It is the employees’ responsibility to ensure that they are at work for 9 hours including one hour lunch break and the given flexibility is not misused.
- Late arrival, early departure or other unplanned absences from scheduled hours are disruptive and must be avoided.

Absences

- If the employee is unable to report to work due to sickness or any other emergency, the Team Lead/Supervisor must be kept informed before 10.00 a.m. on the first day of absence.

Tardiness

- If the employee is reporting to work late due to sickness or any other emergency, the Team Lead/Supervisor must be kept informed. This notification does not excuse the tardiness but simply notifies the stakeholders that a schedule change may be necessary.

- Employees are expected to return from scheduled breaks on time.

Early departures

- Employees who must leave work before the end of their scheduled shift must notify the Team Lead / Supervisor immediately.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR05 Attendance Process

6. Classification

.

☐ Sensitive

☐ Confidential

☑ Restricted

☑ Internal

☐ Public

P-PL03 Meals & Refreshments Policy

1. Purpose

This policy provides guidelines on the provision of meals and refreshments at staff events.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- This policy does not apply to expenses paid from the Xian Club fund.

3. Policy Statements

- The budget should be approved by a member of the leadership team (Management Team, CL Team, Project Lead, Department Manager).
- The budget allocation for a half-day event should be limited to LKR 150/- person (inclusive of taxes).
- The budget allocation for a full-day event should be limited to LKR 700/- person (inclusive of taxes).
- A notice of three working days should be provided to release funds from Finance.
- Internal events of 2-3-hour duration will not qualify for the ordering of refreshments. Exceptional requests will be considered.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR02 Meals & Refreshments Process

6. Classification

.

☐
Sensitive
☐

Confidential

☐

Restricted

☑

Internal

☐

Public

P-PL04 Staff Engagement & Outing Policy

. Purpose

This policy aims at motivating teams and have team building and rewarding at the same time via outings.

2. Scope

2.1 Employment type

This policy is applicable to

☑

All employees

☐

Permanent employees

☐

Probation employees

☐

Contractual employees

☐

Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

Team outings

- Each team is eligible to go for a team outing of their choice quarterly.
- Spending limit for each team member will be Rs.3500/- quarterly. Employees who are shared between more than one project team will get an allocation for each project separately.

Team outings during customer visits

- If a customer visits Sri Lanka, the team can go for an outing (e.g. lunch, dinner) with the customer, in such cases, the spending limit for each team member will be to a maximum of Rs.10,000/- per outing.
- Customer entertainment in the form of excursions will be organized by the company (Inbound Travel Coordinator).
- It is recommended that the services of a professional tour operator should be sought, in order to ensure the health and safety of staff as well as the visiting customers.
- It is the responsibility of the relevant team to decide on the itinerary and obtain necessary approval for the tour and the budget from CEO.
- Upon submission of the approval, the Inbound Travel Coordinator will do the necessary reservations and arrange payments as required.

Virtual team engagements

- In a strictly WFH arrangement (eg: during a pandemic), in order to facilitate team engagement, the team outing budget can be used for virtual team engagement activities.
- Activities should be planned and executed at team level by the delivery lead. Be innovative!
- Types of activities can be (but not limited to) as follows
  - Product release celebrations
  - Virtual Engagement activities
  - Team bonding activities
- All activities should be virtual and not physical, for safety reasons.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL05 Training & Development Policy

1. Purpose

The purpose of this policy is to equip people with the necessary skills, knowledge and attitudes to meet the organization's needs in relation to its objectives.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- Training will be designed and decided based on the Training Needs.
- At least 1 training per employee should be scheduled for a year.
- Training can be local or foreign.
  - To be eligible for training locally, the employee should have served the company for at least six-months.

- To be eligible for training overseas, the employee should have covered at least one year's service. Foreign assignments are decided based on the project and the requirement of the resource.
- All employees should take up foreign assignments with the exception of causes such as pregnancy or any other cause accepted by the management.
- Technology related trainings will be handled within the project and Business, Process and Career related trainings will be handled in organizational level.
- If the company invest on trainings worth above LKR. 30,000 employees are liable to either stay for a minimum period of 1 year or repay the training cost at the time of resignation

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be added.

6. Classification

.

Sensitive

☐
Confidential
☐
Restricted
☑
Internal
☐
Public

P-PL06 Employee Fraternization policy

1. Purpose

99x is an open and friendly workplace and is committed to maintaining an environment in which all Xians, could work together. 99x does not place undue restrictions on employees maintaining close relationships with peers, as it is an individual's right. However, without rules and guidelines relationships between colleagues may negatively impact our workplace. This policy provides a guideline on maintaining workplace conduct and order.

2. Scope

2.1 Employment type

This policy is applicable to

☑
All employees
☐
Permanent employees
☐
Probation employees
☐
Contractual employees
☐

Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

Employee relations at work

- Employees are encouraged to socialize and develop professional relationships in the workplace provided that these relationships do not interfere with the work performance of individuals or with the effective functioning of the workplace. Employees who engage in personal relationships should be aware of their professional responsibilities and will be responsible for assuring that the relationship does not raise concerns about favoritism, bias, ethics and conflict of interest and are advised to talk to their respective Management representative (MR), Corporate Leadership (CL) team member regarding same. *If a relationship has a conflict of interest, actions which could be taken may include, but not limited to, an agreed transfer, a change in reporting structure, or request to resign.*
- Dating colleagues may cause problems if not handled correctly. Examples of common concerns are: Colleagues who date might spend a large portion of their work time talking or meeting with each other instead of completing their duties and engaging with his/her team members. Fights or breakups between couples might affect their ability to collaborate or maintain peace in the workplace. It is advised that employees keep discussions of personal issues out of the workplace and maintain professionalism despite the status of the relationship and seek advice from their Lead, CL member, MR or HR if required.

Unacceptable and Acceptable Behavior

- When employees are in a relationship, it is advised to act appropriately in the workplace. Unacceptable behavior is defined as any action that:
  - Offends fellow Xians.
  - Disrupts or hinders operations.
  - Distracts employees from their duties.
  - Decreases employees' individual performance.
  - Reduces the engagement with other staff and team members
- Examples of unacceptable behavior for employees are:
  - Arguing in the workplace during or after working hours.
  - Displaying affection in front of colleagues at the workplace / company events.

    - Exchanging an excessive number of instant messages or calls unrelated to their work during working hours.
    - Hanging around with your partner, having lunch/tea together.
- Employees are also advised to behave appropriately towards their colleagues who date each other. 99x prohibits victimization and hostility towards employees for any reason. This includes jokes, gossip and improper comments. Employees who witness this kind of behavior should report it to HR.
- All Xians are always obliged to follow the code of conduct.

Openness

- The key point of this policy is openness. As an organization we can't stop employees from forming relationships with one another and trying to prohibit them from doing so could provoke deceit, resentment and gossip. For this reason, we expect all employees to be open about their personal relationships with colleagues. This does not mean that employees should draw attention to their relationship. You can reach out to an MR, CL rep or HR if you need further clarification.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL07 Employee Promotions Policy

1. Purpose

This policy outlines the guideline for advancement and promotion of employees. 99XT believes in investing in employees and rewards all exceptional performances.

2. Scope

2.1 Employment type

This policy is applicable to

☐ All employees

☑ Permanent employees

☐ Probation employees

☐

Contractual employees

Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- Employees may be recommended for a promotion only after being confirmed in the permanent cadre and if they are not under a performance improvement plan.
- Employees will be promoted based on their performance and workplace conduct. The acceptable criteria for a promotion is:
  - The employee should perform at a high level consistently.
    - If being evaluated for the 1st time through the appraisal cycle a score of 95 or above at the concluded appraisal cycle
    - From the 2nd appraisal cycle onwards a minimum average score of 85 in the past two/three appraisal cycles
  - The employee should demonstrate and perform the role of the next level, It should be noted that the competency framework can be used as a guideline to understand the responsibility of the role.
  - The employee should have not been called for an inquiry and or received a warning letter in the last two years.
  - Work experience and tenure in the job role.
- The above criteria depicts an overall view of the employee's performance. Leads should refrain from recommending team members based on recent or insignificant events. It is recommended that leads keep logs with important incidents that they might want to consider when it's time to recommend one of their team members for a promotion.
- The career committee* will not accept promotions based on the leads subjective opinions unsupported by performance appraisal scores, employee fraternization, discrimination, favoritism and nepotism.
- Performance of all employees will be evaluated annually through either the mid year or year-end appraisal cycle. Upon completing the performance appraisal, the team lead should send the promotion recommendations to the Career Committee/ HR via email with a brief description.
- It should be noted that promotion recommendation does not guarantee that the promotion is confirmed and should **NOT** be notified to the employee until the promotion is finalized and confirmed.
- Promotions will be finalized by the Career Committee upon reviewing all employees in the appraisal cycle and will be notified to the employee and lead.

- An employee who wishes to appeal could do so by forwarding a request to the Career Committee via email. The Career Committee would discuss the points stated and notify the employee of the outcome, based on a team vote.

  *The **Career Committee*** comprises of the Management Team relevant Corporate Leadership Team member and HR*

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be added.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL08 Employee Termination Policy

1. Purpose

To ensure that employee terminations, including voluntary and involuntary terminations of an employee, are handled in a professional manner with minimal disruption to the workplace.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- The termination of an employment contract may be categorized as voluntary or involuntary.
- Voluntary termination may include following.
  - Resignation.
  - Retirement.
  - Expiration or completion of contract.
- Involuntary termination may include following.
  - Terminate for cause - Termination due to employees misconduct after a disciplinary action process.
  - Terminate without cause - Discharge without cause can occur when the company decides that the services of an employee are no longer needed. eg: layoffs, rearrangement of a department or redefining of a position.

Voluntary termination

- Employees should provide minimum notice as given below which is also indicated in the conditions of appointment letter/ contract of employment.
  - Permanent and confirmed - 3 months
  - Probationary and contractual employees - 2 months
  - Internship (trainees) - 2 weeks
- Employees are allowed to utilize the current calendar years' annual leave balance to waive off against the notice period.
- Employees are not allowed to utilize the earned annual leave for the following calendar year against the notice period. The earned annual leave will be paid to the employee.

Involuntary termination

- The company should provide notice as per the appointment letter/ contract of employment.

Employee obligations

- Employees shall adhere to the NDA signed to protect the confidentiality and intellectual property rights of all stakeholders. That responsibility and obligation shall survive the termination of the employment contract.
- Employee shall work with the project lead to ensure that the required knowledge transfers are completed within the notice period.
- Utilization of leaves during the resignation notice period depends on the project commitment. This will have to be discussed and mutual agreed with the relevant project lead

- Company provides training to employees with an objective to shape their skills and competency in order for them to perform the duties better. In the event of an employee leaving the company within a year of the training being offered he/she should reimburse the cost incurred on pro rata basis. Refer P-PL05 Training & Development Policy.
- As a part of the project, employees receive opportunities to travel overseas either to client site or to any other location as deemed by the client. This investment is incurred by the client. As an ethical practice, employees resigning 99x within a year from the overseas travel should reimburse the onsite travel cost on pro rate basis to the client. Refer D-PL01 Overseas Travel Policy.
- Employee is required to settle any outstanding company loans before the exit. FI-PL05 Salary Advance Policy (Link Emergency Loans and Off-grid Power Loan policy)
- Employees should return all company properties in their charge and obtain a clearance certificate prior to terminating employment with the company.
- Employee should change any company details stated in their social media profiles after the resignation date.
- Employee should remove him/her self from any work related collaboration tools groups such as Skype, Slack, etc.
- Employee should remove any 99x customer information of any form he/she retains.

General

- According to the Sri Lankan Labour law it is a violation to be employed by two companies at any given time.
- Employees leaving the company should have the opportunity to provide feedback on their employment experience with the company.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR03 Employee Termination Process

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

P-PL09 Remote Work Policy

1. Purpose

This policy outlines the remote work guidelines and scenarios in which remote work will be acceptable

2. Scope

2.1 Employment type

This policy is applicable to

☑

All employees

☐

Permanent employees

☐

Probation employees

☐

Contractual employees

☐

Internship employees

2.2 Other scope elements.

Following remote work scenarios are in scope.

- **Scenario 1** - All employees to work remotely, announcement is made by Management/ HR.
- **Scenario 2** - Hybrid work arrangement, where employees would report to work on an established roster notified by the Management/HR
- **Scenario 3** - Remote work as requested by employee and approved by Management.

3. Policy Statements

- All company policies shall be applicable during remote work scenarios.
- Employees are encouraged to work the standard hours (8) and it is very important to be ethical in time reporting. The actual hours worked should be reported to the time reporting mechanism.
- Employees agree to be accessible and available to be contacted by the management, customers and other relevant stakeholders during the designated working hours as detailed in the contract of employment.
- The employees are expected to respond to any work-related communication within a reasonable period of time.
- The employee shall carry out duties subject to the terms and conditions detailed in the respective employment contract.
- Productivity of employees who work from home shall be measured on factors such as time spent on a specific task, number of matters handled/resolved, number of interactions with clients / co-workers and any other factor that the management may decide and inform at its sole discretion, from time to time.
- Anything which is not covered in this policy should be discussed and approved by a Management Representative.

- Employees must follow all information security norms including physical security while remote working.
- Please refer to the presentation for a detailed outlook on the do's and don'ts when working remotely. <Insert PPT by Madhushan>.

IT Hardware Assets

- Employees are permitted to choose between the following options when sourcing a laptop for remote work.
  - a personal computer could be used after configuring the computer with the security controls by IT Team I-PL04 BYOD Policy
  - a computer rented from a third-party supplier could be used after configuring the computer with the security controls by IT Team. I-PL04 BYOD Policy
  - Note: You may discuss with the IT department to the possibility of purchasing a company owned laptop, based on availability.
- Allocation and collection of IT logistics will be carried out based on the "User Equipment Management During Pandemic"
- Employees should not connect any corporate-provided mobile device to any open/ unknown/ free Wi-Fi networks.
- Remote access to the equipment must not be given to any outsiders other than the IT department.
- If an employee needs to access resources in-office network, VPN access must be approved and provided based on the need.
- At an instance of employee resignation/ termination, the logistics must be returned on the last working day by physically handing over the equipment to office premises or by sending the equipment by courier according to the https://seranet.atlassian.net/wiki/spaces/IT/pages/2950004795
- The employee's device may be remotely wiped if,

a. The device is lost
b. The employee terminates his or her employment
c. IT detects a data or policy breach, a virus or similar threat to the security of the company's data and infrastructure.

Internet Connectivity

- The employee must have a company provided internet facility along with a backup facility from a preferred service provider. At an instance company provided internet connection is not usable the employee can use the personal internet connection and submit a claim.
- The use of company-provided internet facility must be according to the "All Staff Internet Policy for Business Continuity" policy.

- The company has the right to monitor the company-provided equipment/ internet facility and its use.

Intellectual Property

- The employee shall be bound by all legal requirements to protect the information security of the Company and work handled, Intellectual Property Rights as detailed in the NDA.

Confidentiality

- The employee shall be bound by the terms and conditions relating to maintaining confidentiality of all information concerning the businesses of the Company found in the Contract of Employment, Non-Disclosure Agreement, and relevant Policies and Procedures of 99x.

Workmen's compensation / Liability for injuries

- Workman's Compensation Coverage will be limited to the designated workplace as will not cover to adjacent areas, eg. Other areas of the residence.
- The Employer's liability shall be limited to injuries that occurred in the course of or arising out of remote work carried out within the working hours.
- The employee shall personally be liable for injuries caused to third parties and/or any occupier at the Remote Work Location.
- The employee shall indemnify the Employer against any and all claims, demands, and liability, resulting from or arising in connection with, any injury to persons or damage to property, caused directly or indirectly, by the employee's misconduct, negligent acts, or omissions in the performance of the employee's duties and obligations.
- The employee shall immediately report any work-related injury to the Project lead/ Management/HR.
- In the event where the employee is unable to communicate, a family member of the employee shall pass on such a message.
- To ensure the wellbeing of employees the company will establish voluntary confidential counselling sessions which could be arranged with the Company Counsellor (Details can be found on Employee Benefits) or through a telehealth vendor oDoc.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR04 Remote Work Process

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL10 Anti-harassment Policy

1. Purpose

Purpose of this policy is to create an inclusive and collaborative working environment and respect each other at all times.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- All 99x employees have a right to work in an environment free from the demoralizing effects of harassment or unwelcome, offensive or improper conduct.
- While it is not easy to provide a complete list of the types of improper behavior, prohibited conduct certainly includes: sexual harassments, discriminatory acts, bullying and physical violence at work place. Please refer below information panel for details of these acts & behaviors.

  Sexual harassments

- Sexual harassment is considered unwelcome conduct of a sexual nature that is sufficiently persistent or offensive enough to interfere with the receiver's job performance or create an intimidating, hostile or offensive working environment.
- Sexual harassment encompasses a wide range of conduct. Examples of misconduct include, but may not be limited to, the following actions:
  - Physical assaults or the attempt to commit an assault of a sexual nature.
  - Unwelcome sexual advances, propositions or other sexual comments, such as sexually oriented gestures, noises, remarks, jokes, or comments about a person's sexuality or sexual experience.
  - Preferential treatment or promises of preferential treatment to a team member for submitting to sexual conduct.
  - Creating displays, communications, or publications that include content of a sexually offensive nature.

Discrimination

- 99x is committed to the principles of equal opportunity, inclusion, and respect. We do not tolerate discrimination against anyone, including employees, customers, business partners, or other stakeholders. Refer policy on Anti-discrimination.

Bullying / Workplace Violence

- 99x does not tolerate violent acts or threats of violence including following actions.
  - fighting
  - bullying,
  - use of abusive or threatening words.

- We request employees who have either witnessed or faced an incident, to promptly reach out to Shehani (Chief Operating Officer), Damitha (Chief People Officer), or Trudi (Manager HR). As an alternative employees could also report it via Shout Out Box either anonymously or indicating your name.
- All reported incidents will be investigated with an effort to keep the source of the report confidential, except where the company finds disclosure necessary for resolution. Where inappropriate conduct has occurred, specific disciplinary actions, up to and including discharge where appropriate, will be implemented.
- Any employee who, in good faith, reports a possible violation of this policy will be protected from any form of retaliation.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be added

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL11 Anti-discrimination Policy

1. Purpose

The purpose of this policy is to maximize diversity and inclusion within the workplace and to promote equal opportunities.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐ Permanent employees

☐ Probation employees

☐ Contractual employees

☐ Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- 99x values and respects all diverse life experiences within the company culture.
- Discrimination is any negative action or attitude directed toward someone because of protected characteristics, like race and gender. Other protected characteristics might include:
  - Age
  - Religion
  - Ethnicity / nationality

  - Disability / medical history
  - Marriage / civil partnership
  - Pregnancy / maternity/ paternity
  - Gender identity / sexual orientation
- Company will not tolerate any kind of discrimination that creates a hostile and unpleasant environment for employees or any other stakeholders who does business with 99x.
- We recognize that sometimes discrimination is unintentional, as we may all have unconscious biases that could be difficult to identify and overcome. In case we conclude that an employee unconsciously discriminates, we will support them through training and counseling and implement processes that mitigate biases as we indicate in the next section
- We request employees who have either witnessed or faced an incident, to promptly reach out to Shehani (Chief Operating Officer), Damitha (Chief People Officer), or Trudi (Manager HR). As an alternative employees could also report it via Shout Out Box either anonymously or indicating your name.
- All reported incidents will be investigated with an effort to keep the source of the report confidential, except where the company finds disclosure necessary for resolution. Where inappropriate conduct has occurred, specific disciplinary actions, up to and including discharge where appropriate, will be implemented.
- Any employee who, in good faith, reports a possible violation of this policy will be protected from any form of retaliation.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- To be decided.

6. Classification

.

☐ Sensitive
☐ Confidential
☐ Restricted
☑ Internal
☐ Public

P-PL12 Business Cards Policy

1. Purpose

This policy covers the preparation, processing and usage of company business cards.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees
☐ Permanent employees
☐

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- Not applicable.

3. Policy Statements

- Business cards should be issued to all employees at the time of joining the organization.
- Business cards should be issued to existing employees upon a change in the designation.
- Business cards should be issued to existing employees upon special requests from them (eg: to change the information printed on the card, to replenish existing lot, for overseas travelling, etc.)
- Business card printing should be processed mainly in January and August of each year, depending on the number of requests received.
  - Cut-off date for January - 31st January
  - Cut-off date for August - 31st August
- The information, font, color, logo and others formatting mentioned in the business card should be exact or similar to the prescribed format of business card.
- Business cards should not show any personal email addresses.
- At the time of departure, unused cards should be withdrawn and destroyed.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR01 Business Cards Process

6. Classification

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL13 Disciplinary Action Policy

1. Purpose

This policy explains how 99x addresses it's employees' misconduct or inadequate performance and the consequences of such actions.

2. Scope

2.1 Employment type

This policy is applicable to

☑ All employees

☐

Permanent employees

Probation employees

Contractual employees

Internship employees

2.2 Other scope elements.

- Not applicable

3. Policy Statements

- The stages that may be followed when discipline is deemed necessary include the following:
  - Verbal warning
  - Official written reprimand
  - Disciplinary meeting with appropriate supervisor or manager
  - Final written warning
  - Detraction of benefits
  - Indefinite suspension or demotion
  - Termination
- The nature of the offense must be explained to the employee from the beginning of the procedure.
- The following scenarios indicate where the disciplinary procedure starts depending on the violation:
  - **Performance issues** - (e.g., Failure to meet performance objectives., Attendance issues, Failure to meet deadlines, etc.)
  - **One-time minor offense** - (e.g., Rude behavior to fellow employees or customers, On-the-job minor mistakes, Involuntary Discrimination, etc.)
  - **Frequent offender** - (e.g., Lack of response to warnings, Lost temper in front of fellow employees or customers, On-the-job major mistakes, Unwillingness to follow the company standards, etc.)
  - **Severe offensive behavior** - (e.g., Corruption/ Bribery, Breach of employment agreement, Harassment/ Voluntary discrimination, Workplace violence, Fraud, Substance Abuse, etc.)
- 99x Management may choose to repeat stages of the disciplinary procedure as appropriate. This decision depends on employees' reaction to the disciplinary procedure, whether they repent their behavior and the nature of their offense.

- Disciplinary procedure shall begin when there is sufficient evidence to justify it.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- Not applicable.

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public

P-PL13 Substance Abuse Policy

1. Purpose

Being under the influence of alcohol or drugs can impair an individual's judgment and reactions leading to an increased risk of accidents and injuries. Alcohol and drug abuse negatively impact work performance and behavior not only on the person under influence but also on one's work colleagues.

Hence, this policy aims to safeguard 99x employees and its stakeholders against all unacceptable substance abuse to ensure a safe and healthy working environment.

While we have the policy in place, 99x also see the importance of creating an engaging work environment for our fellow Xians, thus allowing Employees to use legal substances as per the policy during approved company events and business gatherings.

2. Scope

2.1 Employment type

This policy is applicable to

- [x] All employees
- [ ] Permanent employees
- [ ] Probation employees
- [ ] Contractual employees
- [ ] Internship employees

2.2 Other scope elements.

- This policy is also applicable for the contractors of 99x.

3. Policy Statements

- All legal/illegal alcohol, illegal drugs, and some inhalants fall into the “unacceptable substances” category.
- Whenever employees are present on 99x work premises or at an offsite work premises conducting company-related, they should not:
  - Possess, use or consume unacceptable substances.
  - Sell, buy, transfer or distribute unacceptable substances or any paraphernalia.
  - Be under the influence of unacceptable substances which may carry the effects over to the working. hours.
  - Smoke tobacco, use e-cigarettes or vape.

Employees who are taking prescription drugs should ensure that they are aware of any side effects and advise their reporting person of any side effects of prescription drugs, which may affect work performance or the health and safety of themselves or others.

Alcohol usage during company events

- Consumption of legal alcohol during company events at designated locations is permitted if the use of alcohol is pre-approved for the event by the Management. Permittable events along with event details such as location and duration of the event will be communicated to the attendees prior to the event.
- Consumption of alcohol should be under the Employees own discretion, in moderation and in a responsible manner.
- Employees who consume alcohol should not compromise the privacy, safety, and liberty of others including fellow Xians at any time.
- Employees should be aware they will be held individually or collectively liable for any detrimental actions/incidents caused under the influence of alcohol.
- Employees should be aware that the company will not be liable for any actions/damages occurring under the influence of alcohol, on or away from the company premises whilst Employees must indemnify the company from all liabilities or damages caused due to the influence of alcohol.
- Employees should be aware that insurance claims identified as being under the influence of alcohol may not be processed favourably by the company insurance partner.
- Employees should not at any time enter the undesignated office premises and/or perform duties under the influence of alcohol or any other substance that result in intoxication.
- When there is a reasonable belief that an individual is under the influence of ‘unacceptable substance’, on reporting for work or during the course of work, they will be sent off the office premises immediately until further actions are carried out related to the matter.

4. Compliance

4.1 Monitoring

Management will verify the policy compliance through various methods, including but not limited to, audits, reviews, periodic walk-throughs, video monitoring, data analysis.

4.2 Exceptions

Any exception to the policy must be handled as per the L-PL20 Exceptions Policy .

4.3 Non Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Processes

- P-PR01 Corporate Events Process

6. Classification

.

☐ Sensitive

☐ Confidential

☐ Restricted

☑ Internal

☐ Public