TELECOM
COMPUTER SOLUTIONS

2024

Code of CONDUCT

5245 HARVESTER ROAD
BURLINGTON, ON
CANADA L7L 5L4

905-333-9621

www.telecomcomputer.com

CCIB
CERTIFIED
INDIGENOUS
BUSINESS

Telecom Computer's Code of Business Conduct

A – Introduction
A - 1.2 Employee Relations Philosophy
A - 1.3 Fair Treatment Policy
A - 1.4 Guiding Principles

B - 1. Workplace Health & Safety
B - 1.1 Occupational Health & Safety Policy
B - 1.2 Mental Health & Well-Being Policy
B - 1.3 Sexual & Other Harassment Policy
B - 1.4 Violence Prevention Policy
B - 1.5 Ergonomics & Workplace Comfort Policy
B - 1.6 Menopause Workplace Support Policy

C - 1. Emergency Preparedness & Response
C - 1.1 Fire Training Policy
C - 1.2 WHMIS (Workplace Hazardous Materials Information System) Policy
C - 1.3 Crisis Management Policy
C - 1.4 Medical Emergency Response Policy
C - 1.5 Evacuation & Shelter-in-Place Policy
C - 1.6 Emergency Closings Policy

D. Safety Compliance & Reporting
D - 1.1 Protective Safety Equipment Policy
D - 1.2 Warehouse Safety Policy
D - 1.3 Office Workplace Safety Policy
D - 1.4 Employee Health & Safety Responsibilities Policy
D - 1.5 Safety & Reporting Accidents Policy
D - 1.6 Hazard Reporting & Resolution Policy
D - 1.7 Return to Work & Injury Management Policy

E - **Cyber & Remote Work Safety**
E - 1.1 Remote Work Health & Safety Policy
E - 1.2 Cybersecurity Awareness & Threat Response Policy

G. Human Rights & Ethical Business Practices
G - 1.1 Human Rights Policy
G - 1.2 Fair Labor Practices Policy
G - 1.3 Indigenous Rights & Reconciliation Policy
G - 1.4 Anti-Discrimination & Equal Opportunity Policy
G - 1.5 Conflict of Interest Policy
G - 1.6 Anti-Corruption Policy

H. Corporate Social Responsibility (CSR) & Environmental Sustainability
H - 1.1 Corporate Social Responsibility (CSR) Policy
H - 1.2 Supplier Code of Conduct
H - 1.3 Environmental Sustainability & Climate Action Policy
H - 1.4 Ethical AI & Data Responsibility Policy

I - **Community Engagement & Social Impact**
I - 1.1 Indigenous Sponsorship & Education Grant Policy
I - 1.2 Employee Volunteerism & Philanthropy Policy
I - 1.3 Ethical Marketing & Customer Responsibility Policy

J - **Workplace Diversity, Equity & Inclusion (DEI)**
J - 1.1 Anti-Discrimination & Equal Opportunity Policy
J - 1.2 Sexual & Other Harassment Policy
J - 1.3 Inclusive Workplace Culture Policy

K - **Indigenous Engagement & Economic Inclusion**
K - 1.1 Indigenous Rights & Reconciliation Policy
K - 1.2 Supplier Diversity & Inclusive Procurement Policy

L - **Accessibility & Workplace Accommodations**
L - 1.1 Disability Inclusion & Workplace Accommodation Policy
L - 1.2 Inclusive Hiring & Advancement Policy

M - **Employee Leaves & Workplace Flexibility**
M - 1.1 General Leaves of Absence Policy
M - 1.2 Bereavement Leave Policy
M - 1.3 Maternity Leave Policy
M - 1.4 Parental Leave Policy
M - 1.5 Emergency Leave Policy
M - 1.6 Flexible Work Arrangements Policy
M - 1.7 Paid Time Off (PTO) Policy

N - **Community & Employee Engagement**
N - 1.1 Employee Volunteerism & DEI Advocacy Policy
N - 1.2 Equal Pay & Pay Transparency Policy

O - **Data Security & Financial Integrity**
O - 1.1 Confidentiality & Data Protection Policy
O - 1.2 Artificial Intelligence (AI) Use & Security Policy
O - 1.3 Email, Internet & IT Usage Policy
O - 1.4 Acceptable Use of Equipment Policy
O - 1.5 Cybersecurity & Threat Prevention Policy
O - 1.6 Security & Access Control Policy
O - 1.7 Insider Trading & Ethical Financial Conduct Policy
O - 1.8 Digital Records Management & Retention Policy
O - 1.9 Third-Party & Vendor Security Policy
O - 1.10 Continuous Monitoring & Improvement Policy

A - Introduction

A - 1.1 Introductory Statement

Telecom Computer Inc. is committed to maintaining a workplace culture that is professional, inclusive, and based on ethical business conduct. This policy framework outlines Telecom Computer's key expectations, employee responsibilities, and corporate commitments to fostering a safe, fair, and productive work environment. The policies outlined in this document are mandatory for all employees, contractors, and business partners and reflect Telecom Computer's commitment to integrity, compliance, and corporate responsibility.

A - 1.2 Employee Relations Philosophy

Telecom Computer Inc. will:

- Comply with all Provincial and Federal laws and company policy obligations related to employee rights.
- Manage employees in a fair, open, and consistent manner while recognizing the needs of both employees and the organization.
- Treat employees with respect, dignity, and professionalism.
- Recruit and retain highly qualified professionals who align with Telecom Computer's values and mission.
- Prioritize internal promotions and professional development opportunities before seeking external hires.
- Ensure equal job opportunities and promote a culture of inclusion.
- Provide ongoing training and career development to enhance employee capabilities and career growth.
- Foster a collaborative and collegial workplace culture where employees are encouraged to share ideas and contribute to business success.

A - 1.3 Fair Treatment Policy

Telecom Computer Inc. is committed to ensuring a fair, transparent, and supportive work environment.

1. Open Communication & Employee Engagement
   - Employees are encouraged to voice concerns, provide feedback, and seek clarification.
   - Supervisors and managers are expected to listen to employee concerns and resolve issues promptly.
   - Employees must treat each other with mutual respect.
2. Problem Resolution Process
   - Discuss with Immediate Supervisor – The employee presents the issue to their supervisor.
   - Escalate to Department Manager – If unresolved, it should be escalated to a senior manager.
   - Review by the President – The President will review the concern and make a final determination.
   - Employees will not face retaliation for reporting concerns in good faith.

A - 1.4 Guiding Principles

Integrity is non-negotiable at Telecom Computer Inc. The company strictly prohibits bribery and corruption.

1. Anti-Bribery & Corruption Policy
   - Employees must not offer, promise, or give anything of value to improperly obtain or retain business.
   - Employees must not accept gifts, favors, or services that create a conflict of interest.
2. Third-Party Accountability
   - Third parties cannot engage in bribery or corruption on Telecom Computer's behalf.
   - Employees must report "red flags" indicating unethical conduct.
3. Transparency & Ethical Recordkeeping
   - All financial transactions must be accurately documented.
   - Misrepresentation of business dealings is strictly prohibited.
4. Compliance with Canadian Laws
   - All business activities must comply with Canadian laws and international regulations.
   - Violations may result in disciplinary action, including termination.

B - 1 Workplace Health & Safety

B – 1.1 Occupational Health & Safety Policy

B – 1.1.1 Purpose

Telecom Computer Inc. is committed to providing a safe, healthy, and hazard-free work environment for all employees, contractors, and visitors. This policy ensures compliance with occupational health and safety laws while fostering a proactive safety culture that prioritizes the well-being of our workforce.

B – 1.1.2 Scope

This policy applies to all employees, contractors, visitors, and business partners at Telecom Computer Inc., including on-site, remote, and field workers.

B – 1.1.3 Responsibilities

B – 1.1.3.1 Management Responsibilities

Telecom Computer Inc. management is responsible for:

- Ensuring compliance with federal, provincial, and local workplace health and safety regulations.
- Providing employees with training, protective equipment, and resources to maintain a safe workplace.
- Conducting regular safety audits, risk assessments, and inspections to identify and mitigate hazards.
- Developing emergency response plans and ensuring all employees are familiar with evacuation procedures.
- Encouraging a culture of safety accountability where employees feel empowered to report hazards.

B – 1.1.3.2 Employee Responsibilities

Employees are responsible for:

- Complying with all health and safety policies, procedures, and workplace regulations.
- Using Personal Protective Equipment (PPE) and safety gear as required.
- Reporting unsafe conditions, hazards, near misses, and workplace incidents to their supervisor or the designated safety officer.
- Participating in mandatory safety training and emergency preparedness drills.
- Following proper ergonomic practices to prevent workplace injuries related to posture, workstation setup, and repetitive strain.

B – 1.1.3.3 Health & Safety Committee

- Telecom Computer Inc. may establish a Health & Safety Committee responsible for monitoring workplace safety, reviewing incidents, and recommending improvements.
- The committee will collaborate with management to ensure compliance with workplace safety regulations and best practices.

B – 1.1.4 Hazard Identification & Risk Assessment

Telecom Computer Inc. commits to identifying and mitigating workplace hazards through:

- Regular safety audits and inspections conducted by trained personnel.
- Incident and near-miss reporting systems to track workplace safety trends.
- Ergonomic assessments for office and remote workstations to prevent musculoskeletal injuries.
- Fire, electrical, and equipment safety checks to ensure compliance with safety standards.

B – 1.1.5 Workplace Safety Training

Employees will receive mandatory occupational health and safety training, which includes:

- Workplace hazard awareness and risk prevention techniques.
- Fire safety and emergency response training.
- WHMIS (Workplace Hazardous Materials Information System) training, where applicable.
- Proper lifting techniques and ergonomics to prevent injuries.
- Cybersecurity safety training for employees working remotely or handling sensitive information.

B – 1.1.6 Emergency Preparedness & Response

Telecom Computer Inc. maintains a comprehensive emergency preparedness plan that includes:

- Fire evacuation procedures, including designated emergency exits and meeting points.
- First-aid response protocols, including access to first-aid kits and trained first responders.
- Workplace violence and active threat response plans.
- Remote work emergency preparedness guidelines, ensuring safety even outside office locations.

B – 1.1.7 Incident Reporting & Investigation

- All workplace accidents, injuries, near misses, and unsafe conditions must be reported immediately.
- An incident investigation process will be conducted to determine root causes and implement corrective actions.
- Employees will not face retaliation for reporting safety concerns in good faith.

B – 1.1.8 Compliance & Disciplinary Actions

Failure to comply with health and safety policies may result in corrective action, disciplinary measures, or termination, depending on the severity of the violation. Compliance will be monitored through audits, safety reports, and ongoing evaluations.

B – 1.1.9. Policy Review & Continuous Improvement

- This policy will be reviewed annually to ensure alignment with industry best practices and legal requirements.
- Telecom Computer Inc. will continually seek innovative safety solutions and invest in workplace wellness initiatives to enhance employee well-being.

B - 1.2 Mental Health & Well-Being Policy

B 1.2.1 Purpose

Telecom Computer Inc. is committed to fostering a healthy, supportive, and inclusive work environment that prioritizes the mental health and overall well-being of all employees. We recognize that mental health is just as important as physical health, and we strive to create a workplace culture where employees feel valued, respected, and supported in maintaining their well-being.

B 1.2.2 Scope

This policy applies to all employees, contractors, and management at Telecom Computer Inc., including on-site, remote, and hybrid workers.

B 1.2.3 Responsibilities

B 1.2.3.1 Employer Responsibilities

Telecom Computer Inc. is committed to:

- Providing a workplace environment that supports mental well-being and work-life balance.
- Reducing mental health stigma by fostering a culture of open dialogue, inclusivity, and respect.
- Ensuring employees have access to mental health resources and wellness initiatives.
- Implementing policies that prevent workplace stress, burnout, harassment, and discrimination.
- Training managers and supervisors to recognize and respond appropriately to mental health concerns.

B 1.2.3.2 Employee Responsibilities

Employees are encouraged to:

- Take an active role in managing their mental health and seeking support when needed.
- Engage in open communication with managers or HR regarding workplace stressors or concerns.
- Respect the mental well-being of colleagues, fostering a supportive and inclusive work environment.
- Utilize available resources and support programs to maintain mental wellness.

B 1.2.4 Workplace Mental Health Support

Telecom Computer Inc. promotes mental health and well-being through the following initiatives:

B 1.2.4.1 Employee Assistance Program (EAP)

- Employees will have access to confidential counseling services to address work-related and personal challenges.
- The EAP provides support for stress, anxiety, depression, financial concerns, grief, substance use, and family matters.

B 1.2.4.2 Flexible Work & Work-Life Balance

- Where possible, the company will provide flexible work arrangements to reduce stress and accommodate personal well-being.
- Encourages employees to disconnect from work outside of business hours and take necessary breaks, vacations, and leaves.

B 1.2.4.3 Manager & Leadership Training

- Managers will receive training on mental health awareness, stress management, and supporting employees facing challenges.
- Leadership will foster a non-judgmental, stigma-free workplace where employees feel comfortable discussing mental health.

B 1.2.4.4 Workplace Stress Management

- Promotes reasonable workloads, clear expectations, and supportive management to prevent workplace stress.
- Encourages a positive work culture that values employee contributions and recognizes achievements.

B 1.2.5 Psychological Safety & Inclusion

- Telecom Computer Inc. commits to maintaining a psychologically safe workplace where employees feel comfortable expressing concerns without fear of retaliation or discrimination.
- Mental health is integrated into diversity, equity, and inclusion (DEI) initiatives to ensure all employees have access to necessary resources.

B 1.2.6 Confidentiality & Non-Retaliation

- All mental health disclosures and support requests will be kept confidential in accordance with privacy laws.
- Employees seeking mental health accommodations or resources will not face discrimination, retaliation, or bias.

B 1.2.7 Accommodations & Leave Support

- Employees experiencing mental health challenges may request reasonable accommodations, including adjusted workloads, remote work, or leave of absence.
- Leave policies, including sick leave, personal leave, and disability leave, apply to mental health conditions just as they do to physical health.

B 1.2.8 Compliance & Continuous Improvement

- Telecom Computer Inc. will comply with all applicable workplace mental health laws and best practices.
- The company will continuously review and improve mental health policies based on employee feedback and industry developments.

B - 1.3 Sexual & Other Harassment Policy

B - 1.3.1 Purpose

Telecom Computer Inc. is committed to maintaining a safe, inclusive, and respectful workplace free from harassment, discrimination, and bullying. This policy is designed to prevent, address, and eliminate harassment in all forms, ensuring that all employees, contractors, and business partners feel valued and protected.

B - 1.3.2 Scope

This policy applies to all employees, contractors, vendors, visitors, and clients who engage with Telecom Computer Inc. It covers all work-related settings, including the physical workplace, remote work environments, work events, business travel, and digital communications.

B - 1.3.3 Prohibited Conduct

B - 1.3.3.1 Definition of Harassment

Harassment includes any unwelcome conduct, whether verbal, physical, or visual, that is based on an individual's sex, race, ethnicity, age, religion, disability, sexual orientation, gender identity, or any other legally protected characteristic. Harassment may involve:

- Verbal: Offensive comments, jokes, insults, slurs, or threats.
- Non-Verbal: Unwelcome gestures, inappropriate images, or suggestive materials.
- Physical: Unwanted touching, blocking movement, or aggressive behavior.
- Digital: Harassment via emails, texts, video calls, or social media.

B - 1.3.3.2 Sexual Harassment

Sexual harassment includes, but is not limited to:

- Unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct of a sexual nature.
- Displaying sexually suggestive objects, pictures, or messages in the workplace.
- Making derogatory comments about a person's appearance, gender, or sexuality.
- Making employment decisions (hiring, promotions, assignments) based on submission to or rejection of sexual advances.

B - 1.3.3.3 Harassment by Third Parties

Employees may also experience harassment from clients, vendors, or the public. If this occurs:

1. Firmly and courteously inform the individual that their behavior is unwelcome.
2. If the behavior persists, report the incident to a supervisor immediately.
3. The company will take appropriate action, up to and including removal or banning of the individual from company premises.

B - 1.3.4 Reporting & Investigation Procedures

B - 1.3.4.1 How to Report Harassment

Employees should report harassment as soon as possible to:

- Their immediate supervisor; or
- The General Manager, if the supervisor is unavailable or if the employee feels uncomfortable reporting to their supervisor.

Reports can be made verbally or in writing, and employees will not face retaliation for making a good-faith report.

B - 1.3.4.2 Investigation Process

- All reports will be taken seriously, handled confidentially, and investigated promptly.
- Investigations will be conducted fairly and impartially, ensuring due process for all parties involved.
- If harassment is confirmed, appropriate corrective action will be taken, which may include training, mediation, disciplinary measures, or termination of employment.

B - 1.3.5 Retaliation Protection

Telecom Computer Inc. strictly prohibits retaliation against employees who report harassment or participate in an investigation. Retaliation includes demotion, termination, unfair treatment, or workplace intimidation. Any retaliation will result in disciplinary action, up to and including termination.

B - 1.3.6 Responsibilities & Prevention Measures

B - 1.3.6.1 Leadership & Supervisor Responsibilities

- Lead by example, fostering a respectful and inclusive workplace.
- Address reports of harassment immediately, ensuring a safe and confidential reporting process.
- Participate in annual harassment prevention training and promote awareness among employees.

B - 1.3.6.2 Employee Responsibilities

- Treat all colleagues, clients, and vendors with respect and professionalism.
- Report any harassment incidents immediately and in good faith.
- Cooperate with investigations and support a positive workplace culture.

B - 1.3.7 Training & Awareness

- Employees and managers will undergo mandatory harassment prevention training as part of their onboarding and ongoing professional development.
- Additional Indigenous Awareness training for all non-indigenous employees has be implemented to promote respect and cultural awareness.

B - 1.3.8 Compliance & Consequences

Anyone found engaging in harassment will be subject to disciplinary action, which may include:

- Mandatory training and corrective action plans.
- Suspension, demotion, or termination of employment.
- Legal consequences if harassment violates applicable laws.

B - 1.4 Violence Prevention Policy

B - 1.4.1 Purpose

Telecom Computer Inc. is committed to providing a safe, secure, and respectful work environment where all employees, contractors, and visitors are protected from violence, threats, and workplace safety risks. The company strictly prohibits workplace violence, harassment, intimidation, and any behavior that could create a hostile work environment.

2. Scope

This policy applies to all employees, contractors, clients, visitors, and vendors at Telecom Computer Inc. It covers all work-related settings, including company offices, remote work environments, client locations, work events, business travel, and digital communications.

3. Definition of Workplace Violence

Workplace violence includes any act or threat of physical violence, intimidation, harassment, or disruptive behavior that occurs in or impacts the workplace. This includes but is not limited to:

3.1 Types of Workplace Violence

- Physical Assault: Hitting, pushing, grabbing, or other physical harm.
- Verbal Threats: Statements that express intent to cause harm.
- Intimidation & Bullying: Aggressive behavior, coercion, or repeated hostile actions that create a fearful or oppressive environment.
- Domestic Violence in the Workplace: Any personal relationship conflict that affects workplace safety.
- Workplace Stalking or Harassment: Unwanted attention, following, or repeated communications causing distress.
- Possession of Weapons: Unauthorized possession of firearms, knives, or dangerous objects on company property.

4. Prevention Measures & Workplace Security

Telecom Computer Inc. will take proactive steps to prevent workplace violence by:

- Establishing a zero-tolerance policy for threats, violence, or aggressive behavior.
- Providing mandatory workplace safety and de-escalation training for employees and managers.
- Conducting workplace security risk assessments to identify and mitigate threats.
- Encouraging employees to report suspicious behavior or security concerns immediately.
- Implementing visitor screening and restricted access policies for office locations.

5. Reporting & Response Procedures

5.1 How to Report Workplace Violence

Any employee who experiences, witnesses, or suspects workplace violence must report the incident immediately to:

- Their immediate supervisor
- The General Manager, if the situation requires escalation or if the supervisor is unavailable

Reports may be made verbally or in writing, and employees will not face retaliation for making a good-faith report.

5.2 Investigation Process

- All reports will be taken seriously, investigated promptly, and handled confidentially.
- The company will conduct a thorough investigation, including interviews and a security risk assessment.
- Corrective action will be taken, which may include disciplinary action, termination, law enforcement involvement, or workplace security enhancements.

6. Emergency Response Plan

In cases of immediate threats or violent incidents:

- Call 911 or emergency services if there is an imminent danger.
- Employees should follow emergency response procedures, including evacuation or lockdown protocols if necessary.
- The General Manager will coordinate response efforts with law enforcement and ensure employee safety.

7. Workplace Safety & Risk Assessment

Telecom Computer Inc. will conduct regular security assessments to:

- Evaluate physical security measures (e.g., controlled access, surveillance, alarm systems).
- Identify potential workplace violence risks and implement prevention strategies.
- Update emergency procedures and provide ongoing employee safety training.

8. Compliance & Consequences

Any employee who engages in workplace violence, threats, or intimidation will face:

- Immediate suspension or termination, depending on the severity of the violation.
- Potential legal action, including police involvement and restraining orders.
- Required participation in workplace violence prevention training before reinstatement (if applicable).

B - 1.5 Ergonomics & Workplace Comfort Policy

1. Purpose

Telecom Computer Inc. is committed to providing a safe, healthy, and comfortable work environment that promotes physical well-being, injury prevention, and productivity. This policy ensures that employees have access to proper ergonomic practices, workplace setup guidelines, and injury prevention measures to reduce the risk of musculoskeletal disorders (MSDs), repetitive strain injuries (RSIs), and other workplace-related health concerns.

2. Scope

This policy applies to all employees, including those working on-site, remotely, or in hybrid work environments. It covers workstations, office furniture, equipment usage, and work habits that affect comfort, posture, and long-term health.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. is responsible for:

- Providing ergonomic workstations, chairs, desks, and equipment to reduce strain and discomfort.
- Conducting ergonomic assessments and workstation evaluations for employees, especially those working long hours at desks or computers.
- Offering guidelines and training on proper posture, workstation setup, and movement breaks.
- Ensuring a safe and comfortable working environment for both in-office and remote employees.

3.2 Employee Responsibilities

Employees are responsible for:

- Following ergonomic best practices when setting up and using their workstations.
- Adjusting their chair height, monitor position, and keyboard placement to reduce strain.
- Taking regular breaks to stand, stretch, and move to prevent fatigue and discomfort.
- Reporting workplace discomfort, pain, or ergonomic concerns to their supervisor or HR.

4. Ergonomic Guidelines for Workstations

4.1 Proper Desk & Chair Setup

- Chair Height: Adjust so feet are flat on the floor, and knees are at a 90-degree angle.
- Back Support: Ensure the chair provides lumbar support to prevent lower back strain.
- Desk Height: Align elbows at a 90-degree angle while typing to avoid wrist strain.
- Monitor Position: Keep the monitor at eye level and an arm’s length away to reduce neck strain.

4.2 Keyboard & Mouse Use

- Keep wrists straight and relaxed while typing or using a mouse.
- Use wrist supports or ergonomic keyboards if necessary.
- Position the mouse close to the keyboard to minimize excessive reaching.

4.3 Screen Time & Eye Health

- Follow the 20-20-20 Rule: Every 20 minutes, look at something 20 feet away for 20 seconds to reduce eye strain.
- Adjust screen brightness and contrast to reduce glare and improve visibility.
- Position monitors to avoid reflections from windows or overhead lights.

5. Injury Prevention & Movement Breaks

- Employees are encouraged to take short breaks every hour to stand, stretch, and move.
- Use sit-stand desks (if available) to alternate between sitting and standing.
- Engage in light stretching or mobility exercises to reduce tension and improve circulation.

6. Remote Work Ergonomics

For employees working remotely:

- The company will provide ergonomic guidelines to help set up a safe home office.
- Employees should ensure adequate lighting, proper seating, and minimal distractions.
- Supervisors may conduct virtual ergonomic assessments if employees report discomfort or concerns.

7. Reporting & Adjustments

- Employees experiencing discomfort, pain, or ergonomic challenges should report them to their supervisor or HR for evaluation.
- The company will assess ergonomic concerns and provide recommendations or adjustments as needed.
- Accommodations will be provided for employees with medical conditions requiring ergonomic modifications.

B - 1.6 Menopause Workplace Support Policy

1. Purpose

Telecom Computer Inc. recognizes that menopause is a natural life stage that can have physical, emotional, and psychological impacts on employees. This policy ensures that employees experiencing menopause are provided with a supportive, inclusive, and accommodating work environment, reducing stigma and enabling them to perform at their best.

2. Scope

This policy applies to all employees who experience menopause, perimenopause, or related health conditions, as well as managers and HR staff responsible for workplace accommodations and employee well-being.

3. Workplace Support & Accommodations

3.1 Reasonable Workplace Adjustments

Employees experiencing menopause symptoms may request reasonable workplace accommodations, including:

- Flexible working arrangements (e.g., adjusted start times, remote work options).
- Access to temperature control (fans, desk adjustments, ventilation improvements).
- Increased access to rest areas and private spaces for symptom management.
- Adjustments to uniforms or dress codes to allow for comfort.

3.2 Health & Well-Being Support

- Employees may take sick leave or emergency leave if menopause-related symptoms significantly impact their ability to work.
- The company will offer confidential HR support for employees needing guidance or accommodations.
- Employees may access mental health resources and wellness programs for additional support.

3.3 Training & Awareness

- Managers and HR staff will receive training on menopause awareness, stigma reduction, and how to support employees.
- The company will promote an inclusive and open culture, ensuring employees feel comfortable discussing workplace needs without fear of discrimination.

4. Request & Approval Process

- Employees seeking workplace adjustments due to menopause symptoms should speak with their manager or HR to discuss accommodations.
- HR will assess requests on a case-by-case basis while ensuring privacy and dignity.
- No employee will face discrimination or retaliation for requesting support related to menopause.

C - 1. Emergency Preparedness & Response

C - 1.1 Fire Training Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring all employees are prepared for fire-related emergencies through proper training and adherence to safety protocols. This policy establishes fire prevention measures, evacuation procedures, and fire safety training requirements.

2. Scope

This policy applies to all employees, contractors, and visitors in company facilities and covers fire safety procedures, evacuation plans, and emergency response measures.

3. Responsibilities

3.1 Employer Responsibilities

- Maintain fire safety equipment, including extinguishers, alarms, and emergency exits.
- Conduct annual fire safety training for all employees.
- Ensure fire exits, routes, and emergency plans are clearly posted.

3.2 Employee Responsibilities

- Participate in mandatory fire safety training.
- Follow evacuation procedures during fire drills or actual emergencies.
- Report fire hazards or malfunctioning equipment to management.

4. Evacuation Procedures

- In case of fire, employees must follow the designated evacuation routes to the nearest exit.
- Do not use elevators during an evacuation.
- Report to the designated assembly point and wait for further instructions.

5. Compliance & Review

- Fire safety procedures will be reviewed annually to ensure compliance with local fire codes and workplace safety laws.
- Employees who fail to participate in fire safety training may face disciplinary action.

C - 1.2 WHMIS (Workplace Hazardous Materials Information System) Policy

1. Purpose

Telecom Computer Inc. ensures employees are trained on the safe handling, storage, and disposal of hazardous materials in accordance with WHMIS regulations.

2. Scope

This policy applies to all employees handling or exposed to hazardous materials within Telecom Computer Inc. facilities.

3. WHMIS Responsibilities

- Employees must complete WHMIS training before handling hazardous substances.
- Safety Data Sheets (SDS) must be read and followed before using chemicals.
- Hazardous materials must be labeled, stored, and disposed of according to WHMIS standards.

4. Compliance & Training

- WHMIS training will be updated annually to reflect any regulatory changes.
- Employees failing to comply with WHMIS safety procedures may face disciplinary action.

Acknowledgment & Agreement

All employees must read, understand, and comply with this WHMIS Policy.

C - 1.3 Crisis Management Policy

1. Purpose

This policy ensures Telecom Computer Inc. has a structured approach to handling crises, including natural disasters, cybersecurity threats, workplace violence, and public health emergencies.

2. Scope

This policy applies to all employees, contractors, and locations, ensuring a coordinated crisis response across the organization.

3. Crisis Response Plan

- A Crisis Response Team (CRT) will be designated to manage crises.
- Employees must follow emergency response protocols for each type of crisis.
- Communication procedures will be activated to inform employees of critical updates.

4. Emergency Response Drills

- Annual crisis management training will be conducted.
- Regular simulation exercises will prepare employees for various emergencies.

5. Compliance & Review

- Crisis response protocols will be reviewed annually.
- Failure to adhere to crisis response procedures may result in disciplinary action.

C - 1.4 Medical Emergency Response Policy

1. Purpose

To ensure a rapid, effective response to medical emergencies, providing first aid and medical assistance as needed.

2. Scope

This policy applies to all employees, contractors, and visitors at Telecom Computer Inc. facilities.

3. Medical Emergency Protocol

- Employees must immediately call 911 in life-threatening emergencies.
- First aid kits are located in designated areas throughout company facilities.
- Employees must report any medical emergencies to their supervisor.

4. First Aid Training & Equipment

- Designated employees will be trained in first aid and CPR.
- Automated External Defibrillators (AEDs) will be available in designated locations.

5. Compliance & Review

- This policy will be reviewed annually.
- Employees must participate in medical emergency response training when required.

C - 1.5 Evacuation & Shelter-in-Place Policy

1. Purpose

To provide a clear, structured plan for evacuating or sheltering in place during emergencies, including fires, natural disasters, workplace threats, or hazardous material spills.

2. Scope

This policy applies to all employees, contractors, and visitors in Telecom Computer Inc. facilities.

3. Evacuation Procedures

- Employees must follow evacuation routes posted throughout company facilities.
- Supervisors must account for their team members at the assembly area.
- Employees must wait for the all-clear signal before re-entering the building.

4. Shelter-in-Place Procedures

- In cases of active threats, severe weather, or external hazards, employees must:
  - Move to designated shelter areas.
  - Lock doors and follow communication updates.
  - Remain sheltered until an all-clear notification is given.

5. Compliance & Review

- Employees must participate in annual evacuation and shelter-in-place drills.

Procedures will be reviewed annually for compliance and effectiveness.

C - 1.6 Emergency Closings Policy

1. Purpose

To establish clear procedures for closing company facilities in the event of severe weather, power outages, public health emergencies, or security threats.

2. Scope

This policy applies to all employees, contractors, and clients affected by emergency closures.

3. Closure Procedures

- The General Manager will determine emergency closures.
- Employees will be notified via email of closures and reopening times.
- Remote work may be required during prolonged closures.

4. Employee Compensation & Responsibilities

- Hourly employees will be paid according to local labor laws.
- Essential employees may be required to report to work or remain on standby.

5. Compliance & Review

- Closure policies will be reviewed annually.
- Employees must follow company instructions during emergency closures.

Conflict of Interest Policy Integration

1. Purpose

To ensure employees act in Telecom Computer Inc.'s best interests, this policy prohibits conflicts between personal, financial, or external business activities and company duties.

2. Scope

This applies to all employees, executives, and board members in situations involving:

- Acceptance of gifts, financial interests, or outside activities
- Relationships with suppliers, customers, or competitors

3. Conflict of Interest Guidelines

3.1 Acceptance of Favours & Gifts

- Employees must not accept gifts, discounts, services, or benefits from business partners without prior approval from the President.
- Bribery or preferential treatment from vendors, suppliers, or customers is strictly prohibited.

3.2 Financial Interests

- Employees must disclose if they have a financial interest in a vendor, supplier, or competitor.
- Any employee ownership in a business dealing with Telecom Computer must be reported to the President.

3.3 Outside Business Activities

- Employees must disclose any external business relationships that could interfere with their role at Telecom Computer Inc.
- Outside employment, consulting, or board memberships must not create conflicts with company duties.

3.4 Media Relations

- Employees must not speak on behalf of Telecom Computer Inc. without prior approval from the President.
- Unauthorized public statements, social media posts, or interviews are strictly prohibited.

4. Compliance & Consequences

- Failure to disclose a conflict of interest may result in immediate termination.
- Employees who violate this policy may face legal consequences and reputational damage.
- All conflicts must be reported to the President for evaluation and resolution.

D - 1.1 Protective Safety Equipment Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring the health and safety of all employees by requiring the proper use of Protective Safety Equipment (PSE). This policy establishes clear guidelines for the use, maintenance, and enforcement of personal protective equipment (PPE) and appropriate work attire to minimize workplace injuries and hazards.

2. Scope

This policy applies to all employees, contractors, and visitors who work in or access high-risk areas, including warehouses, loading docks, technical service areas, and any designated hazardous zones. It covers protective clothing, footwear, and safety gear required for job-specific tasks.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Provide protective safety equipment when required for job functions.
- Conduct risk assessments to determine the appropriate PPE for each role.
- Ensure all employees receive training on the proper use, maintenance, and disposal of protective safety equipment.
- Regularly inspect and replace damaged or worn-out safety equipment.

3.2 Supervisor Responsibilities

Supervisors must:

- Ensure that employees wear the required PPE in designated work areas.
- Monitor compliance and address violations immediately.
- Issue job-specific protective safety equipment to employees and ensure proper usage.
- Report any defective, missing, or improperly used PPE to management for correction.

3.3 Employee Responsibilities

Employees are required to:

- Wear all assigned protective safety equipment as required by their job function.
- Maintain and care for PPE, reporting any damage or need for replacement.
- Follow safety guidelines and procedures when working in high-risk areas.
- Avoid loose-fitting clothing that may pose a safety risk.

4. Protective Safety Equipment Requirements

4.1 General Workplace Safety Equipment

- Closed-toe, slip-resistant footwear is required in warehouses, technical service areas, and storage facilities.
- Employees must wear high-visibility vests when working near moving equipment or vehicles.
- Hearing protection (earplugs or earmuffs) must be used in high-noise environments.

4.2 Job-Specific Protective Equipment

- Warehouse & Logistics Workers
  - Steel-toe boots must be worn when handling heavy materials.
  - Work gloves should be used when lifting, carrying, or handling rough materials.
- Technical Service & Repair Technicians
  - Safety glasses or goggles must be worn when working with electrical or mechanical components.
  - Protective gloves must be worn when handling hazardous substances.
- Employees Working at Heights
  - Fall protection equipment (harness, lanyards) must be used in elevated work areas.
- Chemical Handling & Cleaning Staff
  - Respirators, gloves, and eye protection must be worn when handling hazardous chemicals.

4.3 Prohibited Attire & Unsafe Practices

- Open-toe shoes, sandals, and flip-flops are strictly prohibited in high-risk work areas.
- Loose-fitting clothing, jewelry, and long untied hair must be secured to prevent entanglement in machinery.
- Employees must not alter, remove, or misuse PPE.

5. Training & Enforcement

- Employees will receive training on PPE use and workplace safety procedures upon hiring and annually thereafter.
- Supervisors will enforce compliance, and failure to wear required PPE will result in corrective action or disciplinary measures.
- Employees who fail to comply with PPE policies may face warnings, suspension, or termination, depending on the severity of the violation.

6. Equipment Maintenance & Replacement

- Employees must inspect their PPE before each use and report any damage or wear.
- Telecom Computer Inc. will replace defective or worn-out PPE at no cost to employees.
- Used or contaminated protective gear must be disposed of in accordance with company safety protocols.

7. Compliance & Review

- This policy will be reviewed annually to ensure compliance with occupational health and safety regulations.
- The company will conduct regular safety audits to assess PPE effectiveness and workplace compliance.

D - 1.2 Warehouse Safety Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring a safe and organized warehouse environment by establishing clear safety protocols, housekeeping practices, and operational procedures. This policy minimizes workplace hazards, prevents injuries, and ensures compliance with warehouse safety regulations.

2. Scope

This policy applies to all warehouse employees, contractors, and visitors who enter or work in warehouse facilities. It covers proper housekeeping, machinery safety, hazardous material handling, and employee conduct within the warehouse environment.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Provide safe and well-maintained warehouse facilities.
- Ensure proper storage, signage, and emergency preparedness in all warehouse areas.
- Conduct regular safety training and inspections.

3.2 Supervisor Responsibilities

Supervisors must:

- Ensure employees follow all warehouse safety policies.
- Address and correct safety violations immediately.
- Investigate and report all accidents, injuries, or near-miss incidents.

3.3 Employee Responsibilities

Employees must:

- Follow all warehouse safety procedures and regulations.
- Wear required protective equipment while working in the warehouse.
- Report unsafe conditions, spills, or hazards immediately.

4. Housekeeping & Cleanliness

- Work areas must be kept clean and free of obstructions at all times.
- Spills that present a slipping hazard must be cleaned immediately.
- Tools and equipment must be stored in an organized and secure manner.
- Passageways, aisles, exits, fire protection equipment, and electrical panels must remain clear at all times.

5. Machinery & Personal Safety

- Loose clothing, jewelry, and rings are not permitted while operating machinery.
- Long hair (longer than shoulder-length) must be tied back to prevent entanglement.
- Horseplay, running, and practical jokes are strictly prohibited.
- Employees must never use air hoses to dust off clothing or their body.

6. Material Storage & Handling

- All materials and equipment must be securely stacked to prevent tipping or falling.
- Stored materials must not block walkways, exits, or create tripping hazards.
- Employees must follow proper lifting techniques to avoid back injuries.

7. Reporting Incidents & Hazards

- All injuries, accidents, near misses, unsafe, or potentially hazardous conditions must be reported to a supervisor immediately.
- Employees should report equipment malfunctions or damaged safety equipment as soon as possible.

8. Fire Safety & Emergency Procedures

- Employees must know the location of fire extinguishers, emergency exits, and evacuation routes.
- No smoking is allowed in designated warehouse and flammable material storage areas.
- Fire safety equipment must be accessible at all times.

9. Prohibited Conduct

- Employees must not report to work under the influence of intoxicating or illicit substances.
- Consuming alcohol or drugs on company premises is strictly prohibited and will result in immediate disciplinary action.

10. Training & Compliance

- All warehouse employees will receive mandatory safety training upon hiring and annual refresher courses.
- Failure to comply with warehouse safety policies may result in disciplinary action, suspension, or termination.

11. Policy Review & Continuous Improvement

- This policy will be reviewed annually to ensure compliance with safety regulations and industry best practices.
- Employees are encouraged to provide feedback on warehouse safety improvements.

D - 1.3 Office Workplace Safety Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring a safe, secure, and efficient work environment for all office employees. This policy establishes guidelines for maintaining a clean, organized, and hazard-free office space, while also outlining necessary safety measures for employees who enter the warehouse as part of their job duties.

2. Scope

This policy applies to all office employees, contractors, and visitors at Telecom Computer Inc. It covers general office safety, ergonomics, emergency procedures, and warehouse safety protocols applicable to office personnel.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Maintain a safe and clean office environment.
- Provide ergonomic workstations to reduce strain and injury risks.
- Ensure emergency procedures, exits, and first aid stations are clearly marked and accessible.

3.2 Supervisor Responsibilities

Supervisors must:

- Ensure employees follow office and warehouse safety policies.
- Investigate and report accidents, injuries, or near-miss incidents in the office.
- Encourage a culture of safety awareness and compliance.

3.3 Employee Responsibilities

Employees must:

- Follow all office safety procedures and report unsafe conditions immediately.
- Maintain clean and organized workspaces to prevent hazards.
- Adhere to proper ergonomics and workstation guidelines to prevent strain injuries.

4. Office Safety Guidelines

4.1 Housekeeping & Cleanliness

- Workspaces must be kept free of clutter and obstructions.
- Spills must be cleaned immediately to prevent slips and falls.
- Office aisles, exits, and fire protection equipment must remain clear at all times.
- Personal items (bags, coats, cables) should be stored properly to prevent tripping hazards.

4.2 Ergonomics & Workstation Safety

- Employees should set up their workstations ergonomically to prevent injuries:
  - Chair height and back support should be adjusted for comfort.
  - Monitors should be at eye level to prevent neck strain.
  - Keyboard and mouse placement should minimize wrist stress.
- Employees should take regular breaks to stretch and move.

4.3 Electrical & Equipment Safety

- Employees should ensure cords and power strips are organized and not frayed.
- Only approved electrical devices should be used in the workplace.
- Office equipment (printers, computers, shredders) should be used according to guidelines.

4.4 Fire Safety & Emergency Procedures

- Employees must be familiar with fire extinguisher locations, evacuation routes, and emergency exits.
- In case of a fire, employees should evacuate immediately and report to the designated assembly area.
- No open flames, candles, or smoking are permitted in office areas.

5. Warehouse Safety for Office Employees

As all office employees may enter the warehouse at some point, the following warehouse safety protocols must be followed:

5.1 Entry Requirements

- Office employees must check in with a warehouse supervisor before entering.
- Closed-toe shoes are required when entering the warehouse.
- Employees must stay in designated walkways and follow posted signs.

5.2 Material Handling & Machinery Awareness

- Employees should never operate warehouse equipment (forklifts, pallet jacks, etc.) unless properly trained.
- Stay alert to moving machinery and yield the right of way to warehouse vehicles.
- Avoid leaning on, stacking, or tampering with stored materials.

5.3 Emergency Procedures in the Warehouse

- In case of an emergency, follow warehouse evacuation routes and safety protocols.
- Report any spills, unsafe conditions, or hazards to a warehouse supervisor immediately.

6. Reporting Incidents & Hazards

- Employees must report any injuries, accidents, near misses, or unsafe conditions to their supervisor immediately.
- Supervisors will investigate and take corrective action as needed.

7. Compliance & Review

- This policy will be reviewed annually to ensure compliance with workplace safety laws and best practices.
- Employees failing to follow office or warehouse safety protocols may be subject to disciplinary action.

D - 1.4 Employee Health & Safety Responsibilities Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring a safe and legally compliant work environment by requiring all employees to follow the Occupational Health & Safety Act (OHSA) and related regulations. This policy outlines employee duties and responsibilities under the OHSA to maintain a safe workplace for all.

2. Scope

This policy applies to all employees, contractors, and temporary workers across office, warehouse, and remote work environments.

3. Employee Responsibilities Under the OHSA

3.1 Compliance with the Occupational Health & Safety Act

All employees are required to:

- Work in compliance with the OHSA and its regulations.
- Follow all workplace safety policies and procedures established by Telecom Computer Inc.

3.2 Use of Protective Equipment & Safety Devices

- Use or wear protective equipment, devices, or clothing required by Telecom Computer Inc.
- Report any missing or defective safety equipment that may endanger themselves or others.
- Never remove or disable protective devices, unless authorized and an adequate temporary protective measure is in place.

3.3 Reporting Hazards & Safety Violations

Employees must immediately report to their supervisor or employer:

- Any missing, defective, or unsafe equipment or protective devices.
- Any hazard, dangerous condition, or safety violation in the workplace.
- Any contravention of OHSA regulations or company safety policies.

3.4 Safe Operation of Machinery & Equipment

- No worker shall use or operate any machine, equipment, or tool in a way that may endanger themselves or others.
- Employees must complete required training before operating equipment or handling hazardous materials.

3.5 Prohibited Conduct

The following activities are strictly prohibited as they pose a risk to workplace safety:

- Engaging in horseplay, pranks, contests, or feats of strength.
- Unnecessary running, roughhousing, or reckless behavior in work areas.

4. Enforcement & Compliance

- Failure to comply with this policy or OHSA regulations may result in disciplinary action, suspension, or termination.
- Regular workplace safety audits and employee training will be conducted to ensure compliance.

5. Policy Review & Acknowledgment

- This policy will be reviewed annually to ensure compliance with the latest OHSA regulations.
- Employees must acknowledge and agree to follow this policy as part of their employment responsibilities.

D - 1.5 Safety & Reporting Accidents Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring a safe and healthy work environment for all employees, customers, suppliers, and visitors. This policy establishes guidelines for accident prevention, hazard reporting, and incident investigation, ensuring compliance with the Occupational Health & Safety Act (OHSA) and fostering a proactive safety culture.

2. Scope

This policy applies to all employees, contractors, and visitors at Telecom Computer Inc., covering all workplaces, including offices, warehouses, remote work environments, and customer locations. It defines accident prevention measures, reporting procedures, and corrective actions for workplace incidents.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Comply with the OHSA and all relevant health and safety regulations.
- Take every reasonable precaution to maintain a safe and hazard-free work environment.
- Instruct, train, and supervise employees on safe work practices and procedures.
- Ensure that contractors and subcontractors meet or exceed the company's health and safety standards.
- Provide prompt medical attention and support to any injured employee.
- Investigate all workplace accidents and incidents to prevent recurrence.

3.2 Supervisor Responsibilities

Supervisors must:

- Ensure employees are trained in and follow workplace safety procedures.
- Address and correct hazardous conditions or unsafe practices immediately.
- Investigate and document all reported incidents, near misses, and workplace injuries.
- Work with the Joint Health and Safety Committee (JHSC) to monitor workplace safety.

3.3 Employee Responsibilities

Employees must:

- Work in a safe manner and comply with all company safety rules and procedures.
- Report any hazardous conditions, unsafe equipment, or unsafe work practices to a supervisor immediately.
- Report all workplace injuries, no matter how minor, to their supervisor.
- Participate in safety training and follow safe work practices at all times.
- Cooperate with accident investigations and provide accurate information.

4. Accident & Hazard Reporting Procedures

4.1 Reporting Workplace Injuries

- Any workplace injury, regardless of severity, must be reported immediately to a supervisor.
- If emergency medical attention is required, call 911 immediately, and provide first aid if trained and safe to do so.
- The injured employee and supervisor must complete an Incident Report Form as soon as possible.

4.2 Reporting Unsafe Conditions & Near Misses

- Employees must report any unsafe conditions, hazards, or near misses to their supervisor immediately.
- The supervisor must investigate and correct the hazard promptly.
- Reports can be made verbally or in writing, and employees will not face retaliation for reporting safety concerns.

4.3 Investigating Accidents & Incidents

- All accidents, injuries, and near misses will be investigated by management and the Joint Health & Safety Committee (JHSC).
- Investigations will determine:
  - Root cause of the incident.
  - Corrective actions to prevent recurrence.
  - Whether additional training or process changes are required.
- Investigation findings will be documented and used to enhance workplace safety measures.

5. Emergency Response & Medical Attention

- First aid kits and emergency response procedures will be readily available at all worksites.
- Employees must be aware of emergency contacts and medical assistance locations.
- Supervisors must ensure injured employees receive prompt medical care and complete required workplace injury reports

6. Safety Training & Awareness

- All employees will receive mandatory workplace safety training upon hiring.
- Regular refresher training sessions will be conducted to reinforce safe work practices.
- Safety bulletins, posters, and meetings will promote continuous awareness of workplace safety responsibilities.

7. Enforcement & Compliance

- Failure to report an accident, unsafe condition, or hazard may result in disciplinary action.
- Employees who fail to follow safety procedures or contribute to unsafe work conditions may face corrective action, suspension, or termination.
- Regular workplace safety audits will be conducted to ensure compliance.

8. Joint Health & Safety Committee (JHSC) Role

- The JHSC, composed of employee representatives and management, will oversee the company’s safety program.
- The committee will:
  - Conduct workplace inspections and recommend improvements.
  - Review accident reports and suggest corrective actions.
  - Help develop safety policies and training programs

9. Policy Review & Continuous Improvement

- This policy will be reviewed annually to ensure it aligns with current laws, regulations, and best practices.
- Employee feedback and workplace safety assessments will be used to improve safety programs and procedures.

D - 1.6 Hazard Reporting & Resolution Policy

1. Purpose

Telecom Computer Inc. is committed to maintaining a safe, hazard-free work environment by encouraging employees to identify, report, and resolve workplace hazards in a timely and effective manner. This policy establishes a clear reporting process and outlines how hazards will be assessed and corrected to ensure compliance with the Occupational Health & Safety Act (OHSA) and other applicable workplace safety regulations.

2. Scope

This policy applies to all employees, contractors, and visitors in all work environments, including office spaces, warehouses, remote work locations, and customer sites. It covers physical, chemical, ergonomic, and procedural hazards and ensures proper steps are taken to eliminate risks.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Ensure that employees have a clear process for reporting workplace hazards.
- Take immediate action to investigate, assess, and resolve reported hazards.
- Provide training and resources to employees on hazard identification and prevention.
- Conduct regular workplace inspections to proactively identify risks.

3.2 Supervisor Responsibilities

Supervisors must:

- Encourage employees to report hazards without fear of retaliation.
- Respond promptly to all hazard reports and ensure corrective action is taken.
- Document and track hazard reports and resolutions.
- Work with the Joint Health & Safety Committee (JHSC) to evaluate workplace risks and implement safety improvements.

3.3 Employee Responsibilities

Employees must:

- **Report hazards immediately using the appropriate channels.**
- **Take reasonable precautions to prevent hazards from affecting themselves or others.**
- **Follow all safety procedures and guidelines to reduce workplace risks.**
- **Cooperate with hazard investigations and corrective actions.**

4. Types of Workplace Hazards

Hazards may include, but are not limited to:

4.1 Physical Hazards

- Slips, trips, and fall hazards (wet floors, loose cords, blocked walkways).
- Defective or malfunctioning equipment.
- Fire hazards, including improper storage of flammable materials.

4.2 Chemical Hazards

- Exposure to hazardous substances without proper protection.
- Improper storage or disposal of chemicals.

4.3 Ergonomic Hazards

- Poor workstation setup leading to musculoskeletal issues.
- Repetitive motion injuries from improper equipment use.

4.4 Procedural Hazards

- Lack of proper training for high-risk tasks.
- Failure to follow established safety procedures.

5. Hazard Reporting Process

Step 1: Identify the Hazard

- Any employee who notices a hazardous condition, unsafe behavior, or malfunctioning equipment must take reasonable steps to prevent immediate danger and report it promptly.

Step 2: Report the Hazard

- Employees should report hazards immediately to their supervisor.
- If the hazard is serious and the supervisor is unavailable, the employee must escalate the issue to the General Manager or a Joint Health & Safety Committee (JHSC) representative.
- Hazard reports can be submitted verbally, via email, or using the company's Hazard Report Form.

Step 3: Investigation & Risk Assessment

- Supervisors must investigate all reported hazards within 24 hours.
- The severity, risk level, and potential impact of the hazard will be assessed.
- The JHSC will be involved in high-risk hazard assessments as needed.

Step 4: Corrective Actions & Resolution

- The supervisor or JHSC will determine the appropriate corrective actions, which may include:
  - Removing or repairing hazardous equipment.
  - Modifying work procedures to improve safety.
  - Providing additional employee safety training.
  - Implementing new safety measures or controls.
- Corrective actions must be implemented as soon as possible, with urgent hazards addressed immediately.

Step 5: Documentation & Follow-Up

- All hazard reports and corrective actions will be logged and tracked for continuous improvement.
- The JHSC will review trends in hazard reports to recommend long-term safety improvements.
- Employees who report hazards will receive follow-up communication on resolution actions taken.

6. No Retaliation Policy

- Employees will not face disciplinary action or retaliation for reporting hazards in good faith.
- Any supervisor or manager who discourages reporting will be subject to corrective action.

7. Training & Awareness

- Employees will receive annual training on hazard identification, reporting, and resolution procedures.
- Safety meetings will include discussions on common workplace hazards and prevention strategies.

8. Enforcement & Compliance

- Employees who fail to report known hazards or who willfully create unsafe conditions may be subject to disciplinary action.
- Regular workplace safety audits will ensure compliance with this policy.

9. Policy Review & Continuous Improvement

- This policy will be reviewed annually to align with new safety regulations, workplace risks, and best practices.
- Employee and JHSC feedback will be used to improve hazard reporting systems.

D - 1.7 Return to Work & Injury Management Policy

1. Purpose

Telecom Computer Inc. is committed to supporting employees who experience work-related or non-work-related injuries, illnesses, or mental health conditions, ensuring they receive appropriate recovery time, workplace accommodations, and a structured return-to-work process. This policy ensures that employees recovering from physical injuries, medical conditions, or mental health concerns are provided with the necessary resources to return to work safely and effectively. Additionally, this policy includes ergonomic and remote work accommodations to prevent injuries and support employee well-being, whether in the office, warehouse, or remote work environments.

2. Scope

This policy applies to all employees, including office, warehouse, and remote workers, who:

- Have sustained a work-related or non-work-related injury or illness (physical or mental health-related).
- Require medical or mental health accommodations that impact their ability to work.
- Need ergonomic support to prevent or manage workplace-related health concerns, including those working remotely.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Ensure employees receive appropriate support when needed.
- Develop individualized return-to-work (RTW) plans to facilitate recovery and reintegration.
- Provide ergonomic assessments and accommodations to prevent further injuries.
- Foster an inclusive work environment that supports employees recovering from mental health conditions such as stress, anxiety, or depression.
- Maintain confidentiality regarding employee medical and mental health conditions in compliance with privacy laws.

3.2 Supervisor Responsibilities

Supervisors must:

- Report and document all workplace injuries and incidents, including mental health-related concerns that impact work performance.
- Work with employees, HR, and healthcare providers to develop a safe and gradual return-to-work plan.
- Ensure workplace accommodations are made to support employees with medical or mental health needs.
- Monitor employees returning to work and address any concerns or setbacks with sensitivity and discretion.

3.3 Employee Responsibilities

Employees must:

- Report all injuries, illnesses, or mental health concerns affecting their work to their supervisor or HR.
- Provide medical documentation, when required, supporting their condition and ability to work.
- Participate in rehabilitation, therapy, or treatment plans as recommended by healthcare professionals.
- Follow the agreed return-to-work plan and communicate any difficulties to their supervisor.

4. Injury & Mental Health Management Process

4.1 Reporting an Injury, Illness, or Mental Health Concern

- Employees must immediately report any workplace injury or health-related issue affecting their work to their supervisor or HR.
- If medical or mental health support is required, HR will work with the employee to determine suitable accommodations.
- Employees requesting confidential support for mental health concerns may contact HR or supervisor.

4.2 Workplace Investigation & Prevention

- The Joint Health & Safety Committee (JHSC) and management will investigate incidents to prevent recurrence.
- Recommendations may include changes to workstations, new safety procedures, workload adjustments, or additional training.

4.3 Return-to-Work Plan

A structured RTW plan will be developed in collaboration with the employee, their healthcare provider, and HR. The plan will consider:

- Medical or mental health restrictions and the employee's capabilities.
- Modified work duties, such as reduced hours or adjusted responsibilities.
- Gradual reintegration into full work activities to ensure a successful return.
- Flexible scheduling, remote work options, or workload adjustments as needed.

4.4 Workplace Accommodations

Accommodations may include:

- Adjustments to workstations (ergonomic chairs, standing desks, adjustable monitors).
- Modified schedules, reduced workloads, or hybrid work options to support recovery.
- Additional mental health breaks or wellness resources for employees managing stress, anxiety, or burnout.

5. Remote Work Injury Prevention & Mental Health Support

5.1 Ergonomic Remote Work Setup

Employees working remotely must:

- Use a proper workstation setup to reduce strain (adjustable chair, monitor at eye level, ergonomic keyboard/mouse).
- Take frequent breaks to avoid repetitive strain injuries and reduce mental fatigue.
- Ensure a well-lit, clutter-free, and safe home office environment to support productivity.

5.2 Employer Support for Remote Workers

- Employees may request virtual ergonomic assessments to ensure their home office is safe and comfortable.
- Telecom Computer Inc. will provide mental health resources to help remote workers manage stress and maintain well-being.

6. Compliance & Monitoring

- Employees who fail to report injuries, illnesses, or mental health concerns that affect their work may be subject to corrective action.
- HR will review RTW plans regularly to ensure they remain effective and that employees feel supported.

7. Policy Review & Continuous Improvement

- This policy will be reviewed annually to reflect best practices and regulatory updates.
- Employee feedback will be used to enhance return-to-work, injury prevention, and mental health support strategies.

E - 1.1 Remote Work Health & Safety Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring that employees who work remotely have a safe, ergonomic, and secure work environment. This policy provides guidelines to prevent injuries, support mental well-being, and enhance cybersecurity for remote employees.

2. Scope

This policy applies to all employees working remotely, whether full-time, hybrid, or occasionally from home. It covers:

- Ergonomic workstation setup
- Health, safety, and mental well-being practices
- Cybersecurity and data protection for remote work

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Provide guidelines and resources for setting up an ergonomic home workspace.
- Offer ergonomic assessments upon request to prevent injuries.
- Ensure remote employees have access to mental health and well-being support.
- Provide secure technology and VPN access to protect company data.

3.2 Employee Responsibilities

Remote employees must:

- Set up a dedicated and safe workspace that minimizes distractions and hazards.
- Ensure their workstation is ergonomically sound, including a supportive chair, proper monitor height, and a clutter-free space.
- Take regular breaks to reduce strain and prevent burnout.
- Secure company data by following cybersecurity protocols (e.g., using strong passwords, locking screens when away).

4. Remote Work Safety & Ergonomics

- Workstations should include a desk, ergonomic chair, and appropriate lighting.
- Employees should follow safe posture and positioning recommendations.
- Cords and power strips should be safely arranged to prevent tripping hazards.
- Employees must ensure good internet security practices, including updating software and using company-approved VPNs.

5. Mental Health & Work-Life Balance

- Employees are encouraged to take scheduled breaks and avoid excessive screen time.
- HR will provide access to mental health resources and Employee Assistance Programs (EAPs).
- Communication expectations will be set to prevent employees from feeling the need to be always online.

6. Cybersecurity for Remote Work

- Employees must use company-approved security software and tools when accessing company data.
- Company devices must be password-protected and locked when unattended.
- Employees must never use public Wi-Fi without a company VPN.
- Phishing and scam emails should be reported immediately to IT Security.

7. Compliance & Monitoring

- HR and IT will periodically assess remote work safety and security compliance.
- Employees who fail to follow safety or cybersecurity protocols may be subject to corrective action.

E - 1.2 Cybersecurity Awareness & Threat Response Policy

1. Purpose

Telecom Computer Inc. is committed to protecting company data, customer information, and IT infrastructure by training employees to recognize and prevent cybersecurity threats such as phishing, hacking, and data breaches.

2. Scope

This policy applies to all employees, contractors, and vendors who use company networks, computers, email, and other IT systems.

3. Responsibilities

3.1 Employer Responsibilities

Telecom Computer Inc. will:

- Provide ongoing cybersecurity awareness training for employees.
- Implement strong security controls, including multi-factor authentication (MFA) and encryption.
- Monitor network security and respond to threats immediately.

3.2 Employee Responsibilities

Employees must:

- Complete mandatory cybersecurity training annually.
- Recognize and report phishing emails to IT Security.
- Use strong, unique passwords and enable multi-factor authentication (MFA) where required.
- Never share login credentials or allow unauthorized individuals to access company systems.

4. Cybersecurity Best Practices

4.1 Phishing & Email Security

- Do not open suspicious emails, links, or attachments from unknown senders.
- Report suspected phishing attempts to IT Security.
- Verify unexpected requests for sensitive information before responding.

4.2 Password Security & Access Control

- Use complex passwords with a mix of uppercase, lowercase, numbers, and symbols.
- Never reuse passwords across different accounts.
- Change passwords regularly and never share them with others.

4.3 Data Protection & Secure Communications

- Store company files only on approved cloud platforms or internal servers—never on personal devices.
- Use encrypted messaging and email for sharing confidential information.
- Log out of systems when not in use and lock company-issued devices.

5. Incident Reporting & Threat Response

- If an employee suspects a cybersecurity breach, they must immediately report it to IT Security.
- IT will investigate and take appropriate action, including notifying affected employees or clients.
- Employees who fail to report cybersecurity threats may be subject to disciplinary action.

6. Compliance & Enforcement

- Employees who violate cybersecurity policies (e.g., sharing passwords, clicking on phishing links) may face corrective action, including termination for serious breaches.
- Regular security audits and simulations will be conducted to test cybersecurity readiness.

7. Policy Review & Continuous Improvement

- This policy will be reviewed annually to reflect new threats and best practices.
- IT Security will update employees on emerging cyber risks and necessary precautions.

G - 1.1 Human Rights Policy

1. Purpose

Telecom Computer Inc. is committed to upholding fundamental human rights in all business operations, ensuring that all employees, business partners, and stakeholders are treated with dignity, fairness, and respect. This policy aligns with international human rights standards, including the United Nations Universal Declaration of Human Rights, and aims to prevent discrimination, exploitation, and unethical labor practices.

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties engaged with Telecom Computer Inc. It governs workplace conduct, business operations, and supply chain practices to ensure human rights protections.

3. Core Human Rights Commitments

- Dignity & Respect: All employees and business partners will be treated fairly and without discrimination.
- Freedom from Forced & Child Labor: Telecom Computer Inc. strictly prohibits forced labor, human trafficking, and child labor in any form.
- Right to Safe & Healthy Work Conditions: Employees will be provided with a safe work environment, free from hazards and discrimination.
- Fair Wages & Working Hours: Employees will receive fair compensation in compliance with labor laws.
- Freedom of Association: Employees have the right to form, join, or refrain from joining trade unions or other labor organizations.

4. Reporting Violations

Employees or business partners who witness human rights violations should report them immediately to HR or Compliance. All reports will be confidential and protected from retaliation.

G - 1.2 Fair Labor Practices Policy

1. Purpose

Telecom Computer Inc. is dedicated to fair labor practices, ethical employment standards, and worker rights. This policy ensures that all employees receive fair wages, reasonable working conditions, and equal opportunities.

2. Scope

This policy applies to all employees, contractors, suppliers, and third-party labor providers to ensure ethical employment practices in all operations.

3. Fair Labor Standards

- Compliance with Labor Laws: All employment practices must align with local, national, and international labor laws.
- Fair Wages & Compensation: Employees must be paid fairly in accordance with labor standards, including overtime pay where applicable.
- Reasonable Working Hours: Employees must not be subjected to excessive or exploitative working hours beyond legal limits.
- Non-Discriminatory Practices: Employment decisions will be based on merit, qualifications, and performance, ensuring equal opportunity for all.
- Workplace Grievances: Employees have the right to raise concerns about unfair labor practices without fear of retaliation.

4. Vendor & Supply Chain Compliance

- Suppliers must adhere to fair labor standards and will be audited for compliance.
- Violations of labor laws by suppliers may result in contract termination.

5. Policy Review & Enforcement

- This policy will be reviewed annually for compliance with evolving labor laws and best practices.
- Violations may result in disciplinary action, termination, or legal action.

G - 1.3 Indigenous Rights & Reconciliation Policy

1. Purpose

As an Indigenous-owned company, Telecom Computer Inc. is committed to supporting Indigenous rights, economic inclusion, and cultural reconciliation. This policy ensures respect for Indigenous communities and prioritizes Indigenous procurement, fair business practices, and meaningful partnerships.

2. Scope

This policy applies to all business operations, procurement processes, hiring decisions, and partnerships affecting Indigenous communities. It is aligned with Canada's Truth and Reconciliation Commission's Call to Action #92, which urges businesses to create equitable opportunities for Indigenous peoples.

3. Commitments to Indigenous Rights & Economic Reconciliation

3.1 Cultural Respect & Awareness

- All employees will receive training on Indigenous history, culture, and reconciliation efforts.
- The company will foster an inclusive work environment that recognizes Indigenous perspectives.

3.2 Economic Inclusion & Indigenous Procurement

- Telecom Computer Inc. actively prioritizes legitimate Indigenous businesses in procurement and contracting.
- The company advocates for a procurement structure that ensures legitimate Indigenous businesses are not overshadowed or sidelined by larger firms creating subsidiary entities solely to meet contract requirements.
- Engagement with Indigenous businesses will be based on long-term partnerships, capacity building, and fair opportunities rather than short-term compliance measures.
- The company will promote transparency and accountability in procurement decisions to ensure equitable participation.

3.3 Indigenous Hiring & Workforce Development

- Dedicated programs will support Indigenous hiring, mentorship, and career development within Telecom Computer Inc.
- The company will establish partnerships with Indigenous educational institutions to create pathways for Indigenous students in IT, business, and technology sectors.

3.4 Land & Environmental Responsibility

- Business operations will respect Indigenous land rights and sustainability principles.
- The company will seek Indigenous perspectives on environmental initiatives to ensure responsible and ethical land use.

G - 1.4 Anti-Discrimination & Equal Opportunity Policy

1. Purpose

Telecom Computer Inc. is committed to diversity, equity, and inclusion, ensuring that all individuals receive fair treatment and equal opportunities regardless of race, gender, age, disability, sexual orientation, or Indigenous identity.

2. Scope

This policy applies to all employment practices, including hiring, promotions, training, and workplace culture.

3. Prohibited Discrimination & Harassment

- Employees are protected from discrimination based on legally protected characteristics.
- Sexual harassment, workplace bullying, or discriminatory practices will not be tolerated.

4. Equal Opportunity Commitments

- Merit-based hiring and promotions ensuring fairness for all employees.
- Diversity & Inclusion training for all managers and employees.
- Complaint mechanisms for employees to report discrimination safely.

5. Enforcement & Compliance

- Violations may result in corrective action, termination, or legal consequences.

G - 1.5 Conflict of Interest Policy

1. Purpose

This policy ensures that business decisions are made ethically and free from personal conflicts of interest.

2. Scope

Applies to all employees, contractors, executives, and board members.

3. Identifying & Managing Conflicts of Interest

- Employees must disclose any financial, personal, or family relationships that could interfere with business decisions.
- Accepting gifts, favors, or outside employment that could bias decision-making is prohibited.
- Procurement and hiring must be conducted with fairness and transparency.

4. Disclosure & Enforcement

- Employees must disclose conflicts of interest to management immediately.
- Failure to disclose conflicts may result in disciplinary action or termination.

G - 1.6 Anti-Corruption Policy

1. Purpose

Telecom Computer Inc. is committed to conducting business with integrity and transparency, prohibiting bribery, fraud, and unethical business dealings.

2. Scope

This policy applies to all employees, contractors, suppliers, and business partners.

3. Prohibited Activities

- Bribery & Kickbacks: Employees must not offer, give, or accept bribes, kickbacks, or illegal payments.
- Fraud & Financial Misconduct: All business transactions must be honest, transparent, and legally compliant.
- Improper Influence: Employees must not use their position for personal gain or to unfairly influence business decisions.

4. Reporting & Enforcement

- All suspected corruption must be reported to Compliance immediately.
- Violations will result in corrective action, termination, or legal prosecution.

H - 1.1 Corporate Social Responsibility (CSR) Policy

1. Purpose

Telecom Computer Inc. is committed to operating ethically, sustainably, and with social responsibility, ensuring that our business practices create positive environmental, social, and economic impacts. This Corporate Social Responsibility (CSR) Policy outlines our commitment to ethical business conduct, environmental stewardship, community engagement, and responsible supply chain management.

2. Scope

This policy applies to all employees, suppliers, contractors, and business partners involved in Telecom Computer Inc.'s operations, procurement, and community initiatives.

3. CSR Commitments

3.1 Ethical Business Conduct

- Maintain transparency, accountability, and fairness in all business dealings.
- Ensure compliance with international human rights, labor, and environmental laws.
- Promote diversity, equity, and inclusion across all operations.

3.2 Community Engagement & Indigenous Empowerment

- Support Indigenous economic inclusion through mentorship, sponsorship, and procurement.
- Invest in education, technology access, and STEM programs for underrepresented communities.
- Encourage employee volunteerism and philanthropic efforts.

3.3 Sustainable Business Practices

- Reduce carbon emissions and energy consumption in all operations.
- Implement waste reduction, responsible recycling, and e-waste management.
- Partner with environmentally responsible vendors and suppliers.

4. Policy Compliance & Reporting

- Annual CSR reports will track progress on social and environmental initiatives.
- Employees must uphold CSR principles in their daily work and decision-making.

H - 1.2 Supplier Code of Conduct

1. Purpose

Telecom Computer Inc. is committed to ethical and sustainable sourcing, ensuring that all suppliers meet high standards of labor rights, environmental protection, and business integrity.

2. Scope

This policy applies to all vendors, contractors, and business partners supplying goods and services to Telecom Computer Inc.

3. Supplier Standards

3.1 Labor & Human Rights

- Prohibit child labor, forced labor, and workplace discrimination.
- Ensure fair wages and safe working conditions for all workers.
- Support diversity, equity, and inclusion in hiring and labor practices.

3.2 Environmental Responsibility

- Implement energy-efficient and low-carbon production methods.
- Minimize waste, pollution, and hazardous material use.
- Follow responsible e-waste disposal practices.

3.3 Ethical Business Conduct

- Adhere to anti-bribery, anti-corruption, and fair competition laws.
- Avoid conflicts of interest and unethical business dealings.
- Allow independent audits to verify compliance.

4. Enforcement & Monitoring

- Suppliers must certify compliance with this policy.
- Non-compliance may result in contract termination or corrective action.

H - 1.3 Environmental Sustainability & Climate Action Policy

1. Purpose

Telecom Computer Inc. is committed to reducing environmental impact and supporting global climate action. This policy aligns with our goal of achieving a 1.5-degree reduction in greenhouse gas emissions (Scope 1 & 2) by 2030.

2. Scope

This policy applies to all business operations, employees, suppliers, and partners involved in Telecom Computer Inc.'s supply chain and technology services.

3. Climate & Sustainability Commitments

3.1 Carbon Footprint Reduction

- Reduce energy consumption in data center and office operations.
- Transition to renewable energy sources where feasible.
- Implement sustainable transportation and logistics solutions.

3.2 Responsible Product & Waste Management

- Promote suppliers who develop eco-friendly IT solutions and packaging.
- Prioritize circular economy practices, including product refurbishment and recycling.
- Partner with suppliers who meet environmental sustainability standards.

3.3 Sustainable Procurement & Green IT

- Prioritize environmentally responsible vendors and partners.
- Invest in green IT solutions, including low-energy servers, sustainable cloud computing, and biodegradable materials.
- Reduce e-waste through IT asset lifecycle management and responsible disposal.

4. Tracking & Compliance

- Annual sustainability reports will monitor emissions reductions and sustainability initiatives.
- Employees and suppliers must adhere to green business practices and seek continuous improvement in sustainability efforts.

H - 1.4 Ethical AI & Data Responsibility Policy

1. Purpose

As a technology-focused company, Telecom Computer Inc. is dedicated to ensuring that Artificial Intelligence (AI) and data-driven solutions are used responsibly, ethically, and securely. This policy establishes guidelines for ethical AI use, data privacy, and bias prevention to protect users, clients, and communities.

2. Scope

This policy applies to all AI-driven tools, machine learning applications, and data processing activities within Telecom Computer Inc.

3. Ethical AI & Data Protection Standards

3.1 AI Ethics & Fairness

- Ensure AI tools do not promote bias, discrimination, or misinformation.
- Use transparent AI models that provide explainable and fair outcomes.
- Follow international AI governance standards (e.g., OECD AI Principles, EU AI Act).

3.2 Data Security & Privacy

- Protect customer and employee data in compliance with GDPR, PIPEDA, and industry standards.
- Avoid entering sensitive or confidential company data into public AI models.
- Implement multi-layered security protections for AI-driven systems.

3.3 Responsible AI Innovation

- Use AI to enhance efficiency, security, and responsible automation.
- Perform regular audits of AI models to ensure compliance with ethical guidelines.
- Educate employees on AI risks, limitations, and ethical concerns.

4. Compliance & Enforcement

- Employees must report AI misuse or security risks to IT and Compliance.
- Violations may result in corrective actions, including access restrictions or disciplinary measures.
- This policy will be reviewed annually to adapt to emerging AI and data protection regulations.

I - 1.1 Indigenous Sponsorship & Education Grant Policy

1. Purpose

As an Indigenous-owned company, Telecom Computer Inc. is committed to empowering Indigenous youth by providing mentorship, sponsorship, and education grants to support their success in the fields of Information Technology, Computer Science, and Business Development. This policy ensures that Indigenous students receive the resources, training, and opportunities needed to thrive in the technology industry while also advocating for increased job opportunities in remote Indigenous communities.

2. Scope

This policy applies to Indigenous students, employees, and community partners who are eligible for sponsorships, scholarships, and educational programs.

3. Commitments to Indigenous Education & Economic Growth

3.1 Indigenous Sponsorship & Grant Programs

- Telecom Computer Inc. will allocate annual funding for scholarships and educational grants to Indigenous students.
- The company will partner with larger organizations to expand job opportunities and resources into remote Indigenous communities, ensuring equitable access to employment and career development across all sectors.
- Telecom Computer Inc. will advocate for and sponsor internships within the ICT industry, encouraging industry leaders to provide Indigenous youth with career-building experiences in technology and business roles.

3.2 Community Partnerships & Support

- Telecom Computer Inc. will collaborate with Indigenous communities and leaders to tailor education grants and career programs that address specific community needs.
- The company will prioritize Indigenous students and entrepreneurs in sponsorship opportunities for industry conferences, training programs, and professional development initiatives.

4. Application & Selection Process

- Eligible Indigenous students may apply for scholarships and grants through an annual application process.
- Selection will be based on academic performance, leadership potential, and community impact.

5. Policy Review & Reporting

- The program’s impact and effectiveness will be assessed annually, with opportunities for expansion based on community needs.
- Reports will be shared with Indigenous business councils and community partners to ensure transparency and effectiveness.

I - 1.2 Employee Volunteerism & Philanthropy Policy

1. Purpose

Telecom Computer Inc. encourages employees to actively participate in community engagement and diversity, equity, and inclusion (DEI) initiatives. This policy provides guidelines for volunteer opportunities, corporate-sponsored service projects, and DEI advocacy efforts, empowering employees to make a positive social impact while aligning with the company's values and mission.

2. Scope

This policy applies to all employees and covers:

- Volunteer activities
- Corporate philanthropy
- DEI advocacy and leadership
- Community service participation

3. Volunteerism & Community Engagement

3.1 Paid Volunteer Days

- Employees are eligible for up to two paid volunteer days per year to participate in their own community service efforts, environmental projects, or charitable initiatives.
- Volunteer activities must align with Telecom Computer Inc.'s CSR and DEI commitments.

3.2 Corporate-Sponsored Volunteer Programs

- Telecom Computer Inc. will organize annual volunteer opportunities, such as:
  - Environmental sustainability projects (e-waste recycling, tree planting, clean-up drives).
  - Indigenous community initiatives (mentorship programs, economic development support).

3.3 Employee-Initiated Volunteering

- Employees may propose volunteer projects that align with company values.
- HR will review and approve proposals based on impact, feasibility, and company priorities.

4. DEI Advocacy & Employee Engagement

4.1 Diversity & Inclusion Leadership

- Employees are encouraged to champion DEI initiatives by participating in:
  - DEI training, panels, and awareness campaigns.
  - Industry partnerships that promote diversity in technology.

4.2 Mentorship & DEI Programs

- The company will provide resources and training to support mentorship and advocacy efforts that align with Telecom Computer Inc.'s CSR and DEI commitments.

5. Request & Approval Process

- Employees must submit volunteer requests to HR at least two weeks in advance.
- Requests will be reviewed based on business needs and alignment with corporate values.
- Employees are responsible for ensuring that volunteer work does not interfere with core job responsibilities.

6. Compliance & Policy Review

- This policy will be reviewed annually to ensure it reflects current volunteerism trends, DEI advancements, and business priorities.
- Employees are encouraged to share feedback to improve volunteer and DEI engagement opportunities.

I - 1.3 Ethical Marketing & Customer Responsibility Policy

1. Purpose

Telecom Computer Inc. is committed to transparent, ethical, and responsible marketing that promotes digital accessibility, customer trust, and fair business practices. This policy ensures that all advertising, branding, and customer interactions align with honesty, inclusion, and corporate integrity.

2. Scope

This policy applies to all marketing, sales, advertising, and customer service activities, including digital, print, and social media communications.

3. Ethical Marketing Standards

3.1 Truthful & Transparent Advertising

- All marketing materials must be honest, accurate, and free from misleading claims.
- The company will not engage in deceptive advertising, false product claims, or predatory sales tactics.

3.2 Digital Accessibility & Inclusive Customer Communication

- All digital content, websites, and customer portals will be designed for accessibility, ensuring usability for individuals with disabilities.
- Telecom Computer Inc. will comply with Web Content Accessibility Guidelines (WCAG) to provide an inclusive online experience.
- Customer service teams will be trained in culturally sensitive and inclusive communication practices.

3.3 Ethical Data Usage & Consumer Privacy Protection

- The company will not sell or misuse customer data for unethical marketing purposes.
- Customer data collection will comply with GDPR, PIPEDA, and global privacy laws.

J - 1.1 Anti-Discrimination & Equal Opportunity Policy

1. Purpose

Telecom Computer Inc. is committed to diversity, equity, and inclusion by ensuring that all individuals receive equal treatment and opportunities in the workplace. This policy reinforces our commitment to a work environment free from discrimination, bias, and systemic barriers while expanding on our existing Sexual & Other Harassment Policy.

2. Scope

This policy applies to all employees, contractors, applicants, vendors, and business partners across all company locations, including remote work environments.

3. Prohibited Discrimination & Harassment

Telecom Computer Inc. prohibits discrimination based on:

- Race, ethnicity, or national origin
- Gender, gender identity, or gender expression
- Sexual orientation
- Disability (visible and non-visible)
- Age, marital status, or family status
- Religious beliefs or cultural identity
- Indigenous identity
- Any other legally protected characteristics

All employment decisions—including hiring, promotions, training, compensation, and workplace assignments—must be based on merit, qualifications, and business needs, ensuring fairness and equity.

4. Equal Opportunity Commitments

- Merit-Based Hiring & Promotions: All roles are filled based on skills, qualifications, and experience.
- Reasonable Workplace Accommodations: The company will provide accommodations for employees with disabilities or unique needs.
- Training & Development: All employees and managers will receive DEI training to recognize and prevent discrimination.
- Zero-Tolerance Policy for Discrimination & Retaliation: Employees are protected from retaliation for reporting concerns or participating in investigations.

5. Complaint & Reporting Process

- Employees experiencing or witnessing discrimination must report incidents to HR or a designated DEI representative.
- Reports will be investigated confidentially, and corrective actions will be taken if necessary.

J - 1.2 Sexual & Other Harassment Policy

1. Purpose

Telecom Computer Inc. is dedicated to maintaining a safe, respectful, and harassment-free workplace. This policy expands upon our existing Sexual & Other Harassment Policy by reinforcing expectations, prevention strategies, and reporting mechanisms.

2. Scope

This policy applies to all employees, contractors, customers, vendors, and visitors interacting with Telecom Computer Inc.

3. Definition of Harassment

Harassment includes unwelcome conduct that creates an intimidating, hostile, or offensive work environment, including but not limited to:

- Sexual Harassment: Unwanted sexual advances, inappropriate comments, suggestive jokes, or pressure for sexual favors.
- Verbal & Physical Harassment: Derogatory comments, threats, or offensive gestures.
- Discriminatory Harassment: Any behavior that targets an individual based on protected characteristics such as race, gender, disability, or religion.
- Cyber Harassment: Unacceptable conduct through emails, social media, or workplace communication platforms.

4. Preventive Measures

- Mandatory Anti-Harassment Training: All employees must complete harassment prevention training annually.
- Managerial Accountability: Supervisors must actively enforce anti-harassment policies and respond to complaints promptly.
- Bystander Intervention Training: Employees are encouraged to safely intervene or report harassment when witnessed.

5. Reporting & Investigation Process

- Employees experiencing harassment should report incidents immediately to HR or their manager.
- Anonymous reporting options will be available for employees who do not feel comfortable coming forward directly.
- Reports will be investigated confidentially and without retaliation.

6. Consequences for Violations

- Employees found engaging in harassment may face corrective action, suspension, or termination.
- Customers, vendors, or contractors engaging in harassment may be restricted or banned from doing business with the company.

J - 1.3 Inclusive Workplace Culture Policy

1. Purpose

Telecom Computer Inc. fosters a culture of inclusion, belonging, and diversity where every employee feels valued, supported, and empowered. This policy establishes the framework for creating a diverse and welcoming workplace that encourages collaboration and innovation.

2. Scope

This policy applies to all employees, leadership, contractors, and business partners in all work environments, including remote teams.

3. Commitments to Workplace Inclusion

3.1 Building an Inclusive & Respectful Culture

- Employees are expected to respect differences in perspectives, backgrounds, and experiences.
- The company will recognize and celebrate cultural and identity-based events to foster awareness and appreciation of diversity.
- All employees will have equal access to leadership opportunities and mentorship programs.

3.2 Inclusive Communication & Collaboration

- Use of Inclusive Language: Employees should use gender-neutral and culturally sensitive language in communications.
- Respect for Pronouns & Identities: Employees must acknowledge and respect colleagues' chosen names and pronouns.
- Accommodating Religious & Cultural Observances: The company will provide flexibility for employees observing religious or cultural holidays.

3.3 Supporting Employee Resource Groups (ERGs)

- Employees will have the opportunity to form and participate in Employee Resource Groups (ERGs) based on shared identities, interests, and experiences.
- ERGs will be supported by company leadership and given resources to promote diversity initiatives.

3.4 Diversity in Leadership & Hiring

- Hiring panels will be trained in unconscious bias mitigation to ensure equitable recruitment processes.
- The company will actively seek diverse candidates for leadership and executive roles.

4. Accountability & Continuous Improvement

- The company will conduct annual DEI audits to measure progress in creating an inclusive work environment.
- Employee feedback will be collected to identify areas for improvement in workplace inclusion initiatives.
- Leadership will be held accountable for fostering a culture of inclusion, with DEI metrics integrated into performance evaluations.

K - 1.1 Indigenous Rights & Reconciliation Policy

1. Purpose

As an Indigenous-owned company, Telecom Computer Inc. is committed to Indigenous economic empowerment, reconciliation, and meaningful inclusion in all aspects of our operations. This policy builds on our Corporate Social Responsibility (CSR) and Diversity, Equity & Inclusion (DEI) initiatives to ensure that our business practices actively support Indigenous rights, economic development, and cultural awareness.

2. Scope

This policy applies to all employees, leadership, suppliers, business partners, and procurement processes at Telecom Computer Inc. It governs hiring, procurement, corporate partnerships, and internal reconciliation efforts.

3. Commitments to Indigenous Rights & Economic Inclusion

3.1 Supporting Indigenous Economic Growth

- Investing in Indigenous-led projects, innovation, and entrepreneurship initiatives to promote long-term economic sustainability.
- Advocating for a procurement structure that ensures that legitimate Indigenous businesses are not overshadowed by larger firms creating subsidiary entities solely to meet contract requirements.

3.2 Promoting Indigenous Hiring & Workforce Development

- Actively recruiting Indigenous employees for roles in IT, business management, and leadership.
- Providing mentorship, training, and career development tailored to Indigenous professionals.
- Supporting Indigenous youth education programs through partnerships, scholarships, and sponsorships.

3.3 Cultural Awareness & Reconciliation Initiatives

- Requiring Indigenous Awareness training for all non-indigenous employees to enhance awareness and respect for Indigenous perspectives.
- Recognizing and observing Indigenous cultural events within company operations.
- Engaging with Indigenous communities to guide reconciliation efforts.

4. Compliance & Accountability

- Annual audits will assess progress in Indigenous hiring, procurement, and reconciliation initiatives.
- Leadership will be held accountable for ensuring Indigenous engagement goals are met.

K - 1.2 Supplier Diversity & Inclusive Procurement Policy

1. Purpose

Telecom Computer Inc. is committed to creating an equitable supply chain that supports Indigenous and diverse businesses. This policy ensures that our procurement practices align with Indigenous Procurement and DEI goals, promoting economic inclusion, fairness, and long-term partnerships with underrepresented suppliers.

2. Scope

This policy applies to all supplier relationships, procurement processes, vendor partnerships, and contract negotiations across Telecom Computer Inc.'s business operations.

3. Supplier Diversity Commitments

3.1 Indigenous & Minority-Owned Business Inclusion

- Increase internal spend with Indigenous & Minority-Owned Business businesses.
- champion the need for greater accountability in joint ventures, subcontracting agreements, and partnerships, ensuring that the benefits designated for Indigenous partners are properly distributed and reach them as intended.
- Advocate that minority-owned, women-owned, and underrepresented businesses have fair access to procurement opportunities.

3.2 Ethical & Inclusive Procurement Standards

- Vendors must adhere to ethical labor, sustainability, and anti-corruption standards.
- Telecom Computer Inc. will actively engage with Indigenous business councils, supplier diversity networks, and minority supplier development programs to expand our inclusive supply chain.
- Regularly review and audit supplier diversity performance to ensure alignment with company goals.

3.3 Indigenous Procurement Advocacy

- Advocate for government and corporate policies that strengthen Indigenous procurement opportunities.
- Oppose the creation of artificial Indigenous subsidiaries by non-Indigenous firms attempting to meet contract requirements without genuine Indigenous participation.
- Collaborate with Indigenous businesses and advocacy groups to promote fair competition and economic sustainability.

4. Compliance & Monitoring

- Telecom Computer Inc. will track and publicly report on supplier diversity performance.
- Non-compliance with ethical procurement or diversity standards may result in contract termination.

L - 1.1 Disability Inclusion & Workplace Accommodation Policy

1. Purpose

Telecom Computer Inc. is committed to creating an accessible and inclusive workplace where employees with disabilities have equal opportunities, reasonable accommodations, and full participation in all aspects of employment. This policy ensures that employees and job applicants with disabilities receive the necessary accommodations and support to perform their roles effectively while promoting a culture of accessibility and inclusion.

2. Scope

This policy applies to all employees, job applicants, contractors, and business partners at Telecom Computer Inc., covering hiring, workplace accommodations, career advancement, and accessibility initiatives.

3. Commitments to Disability Inclusion

3.1 Workplace Accessibility & Reasonable Accommodations

- Provide reasonable accommodations for employees with disabilities to ensure they can perform their job functions effectively.
- Ensure all company facilities, workspaces, and digital platforms are designed to be accessible.
- Implement assistive technologies, accessible workstations, and flexible work arrangements to support employees with disabilities.

3.2 Equal Opportunity & Fair Treatment

- Employees with disabilities will be evaluated based on skills, experience, and performance, ensuring equal opportunity for hiring and promotions.
- Disability status will not affect career progression, compensation, or employment benefits.
- Employees with disabilities will have equal access to training, leadership programs, and professional development.

3.3 Digital Accessibility & Inclusive Technology

- Ensure that all internal software, websites, and customer platforms comply with Web Content Accessibility Guidelines (WCAG).
- Provide employees with accessible communication tools, screen readers, and speech-to-text software as needed.

4. Requesting Accommodations

- Employees or job applicants requiring accommodations must submit a formal request to HR.
- HR will engage in an interactive process to assess and implement accommodations.
- Confidentiality will be maintained throughout the process, and no employee will face retaliation for requesting accommodations.

L - 1.2 Inclusive Hiring & Advancement Policy

1. Purpose

Telecom Computer Inc. is committed to fair, inclusive, and unbiased hiring and promotion practices that provide equal opportunities for all employees. This policy ensures that hiring, promotions, and leadership opportunities are based on merit, qualifications, and performance—free from discrimination, bias, or systemic barriers.

2. Scope

This policy applies to all hiring, promotion, and career advancement decisions within Telecom Computer Inc., covering employees, job applicants, and leadership roles.

3. Fair & Inclusive Hiring Practices

- Job descriptions, postings, and application processes will be designed to attract diverse talent.
- Unbiased hiring panels will be trained to mitigate unconscious bias in recruitment and interviews.
- Resumes and applications will be screened using objective evaluation criteria that focus on qualifications, experience, and skills.

4. Career Advancement & Leadership Development

- All employees, regardless of gender, disability, ethnicity, or background, will have equal access to leadership roles and promotions.
- Performance evaluations will be conducted fairly, based on clear, measurable performance indicators.
- Leadership development programs will prioritize diverse talent pipelines to ensure equal representation in senior roles.

5. Pay Equity & Fair Compensation

- Salary structures and compensation practices will be reviewed to ensure pay equity across all roles.
- Employees will receive transparent feedback on promotion and advancement decisions to maintain fairness.

6. Training & Awareness

- All employees, including hiring managers and executives, will receive training on inclusive hiring practices, bias reduction, and equitable career advancement.
- Employee mentorship programs will be established to support career growth for underrepresented groups.

M - 1.1 General Leaves of Absence Policy

1. Purpose

Telecom Computer Inc. recognizes that employees may face pressing personal circumstances that require time away from work. This policy provides guidance on unpaid leaves of absence, ensuring a fair and consistent process while maintaining business continuity.

2. Scope

This policy applies to all full-time and part-time employees who may need to request a temporary unpaid leave of absence due to personal, medical, or religious reasons.

3. Leave of Absence Guidelines

3.1 Unpaid Leave of Absence

- Employees may apply for an unpaid leave of absence for up to 30 days in cases of urgent personal circumstances.
- All requests will be assessed based on business needs and operational impact.
- Approval is subject to management discretion and will be granted on a case-by-case basis.

3.2 Religious Holidays & Cultural Leave

- Telecom Computer Inc. recognizes the diverse cultural and religious backgrounds of its workforce.
- Employees wishing to observe religious holidays may request:
  - A leave of absence without pay, or
  - The use of a vacation day to accommodate their observance.
- Requests for religious leave should be made in advance to allow for proper scheduling.

3.3 Benefits Continuation During Leave

- Employees on an approved leave of absence may continue their participation in the company's benefit plan under the following conditions:
  - The employee must cover both the employer and employee contributions to the benefit package.
  - Payments must be made monthly, in advance, via cheque.
  - If the employee fails to provide payment, benefits will be canceled immediately.

4. Request & Approval Process

- Employees must submit a formal leave of absence request to their manager or HR department, stating:
  - The reason for the leave,
  - The requested duration, and
  - Any special accommodations needed.
- HR and management will review requests based on business needs and fairness in policy application.

5. Compliance & Policy Review

- This policy will be reviewed annually to ensure alignment with labor laws and workplace needs.
- Employees are encouraged to consult HR for any clarification regarding leave entitlements.

M - 1.2 Bereavement Leave Policy

1. Purpose

Telecom Computer Inc. recognizes the emotional and practical challenges that come with the loss of a loved one. This policy provides employees with paid bereavement leave to allow time for grieving, attending funeral services, and making necessary arrangements.

2. Scope

This policy applies to all full-time and part-time employees experiencing the loss of an immediate family member.

3. Bereavement Leave Entitlements

3.1 Immediate Family Members (Three Days of Paid Leave)

Employees are entitled to up to three scheduled working days of paid leave for the death of an immediate family member, which includes:

- Spouse or same-sex partner
- Child or stepchild
- Parent or stepparent
- Brother or sister
- Stepbrother or stepsister

The purpose of this leave is to attend the funeral and/or make funeral arrangements.

3.2 Extended Family Members (One Day of Paid Leave)

Employees are entitled to one scheduled working day of paid leave for the death of the following family members:

- Grandparent
- Current mother-in-law or father-in-law
- Brother-in-law or sister-in-law

4. Additional Leave Considerations

- If additional time is needed, employees may request vacation days or an unpaid leave of absence.
- Employees may also request flexible work arrangements to accommodate travel or personal grieving needs.

5. Request & Approval Process

- Employees must notify their manager or HR as soon as possible when requesting bereavement leave.
- Proof of bereavement (e.g., obituary, funeral program) may be requested at the discretion of HR.

6. Compliance & Policy Review

- This policy will be reviewed annually to ensure it meets employee needs and remains aligned with labor laws.
- Employees should contact HR for clarifications or additional support during their bereavement period.

M - 1.3 Maternity Leave Policy

1. Purpose

Telecom Computer Inc. is committed to supporting employees during pregnancy and childbirth by providing an unpaid maternity leave of absence in accordance with the Employment Standards Act (ESA). This policy outlines the eligibility, duration, and rights of employees taking maternity leave.

2. Scope

This policy applies to all eligible employees who have been employed by Telecom Computer Inc. for at least 13 weeks preceding the expected date of delivery.

3. Maternity Leave Entitlements

3.1 Duration & Timing of Leave

- Eligible employees are entitled to 17 weeks of unpaid maternity leave.
- Maternity leave cannot begin earlier than 17 weeks before the expected date of delivery.
- If the pregnancy ends in a stillbirth or miscarriage, the 17-week maternity leave period does not apply.

3.2 Notice Requirements

- Employees must provide at least two weeks' written notice before the maternity leave begins.
- A medical certificate confirming the estimated due date must be submitted with the request.
- In cases of pregnancy complications or premature birth, the two-week notice requirement may be waived.
- If an employee does not specify an end date, it will be assumed that they will take the full 17 weeks of maternity leave.

3.3 Returning to Work

- Employees who wish to return earlier or extend their leave within the 17-week period must provide at least four weeks' written notice before their expected return date.
- Employees returning from maternity leave will be reinstated to their previous position or an equivalent role with no loss of seniority.

4. Benefits & Seniority During Leave

4.1 Benefits Continuation

- Employees on maternity leave may choose to continue participating in the company's benefit plan by covering both the employer and employee contributions.
- Payments must be made monthly, in advance, via cheque.
- If the employee fails to provide payment, benefits will be canceled immediately.

4.2 Seniority & Employment Rights

- Seniority will continue to accrue throughout the maternity leave period.
- Employees on maternity leave retain all rights to employment benefits, salary adjustments, and promotional opportunities upon their return

5. Request & Approval Process

- Employees must submit a formal maternity leave request to HR with the necessary documentation.
- HR will review requests to ensure compliance with ESA regulations.

6. Compliance & Policy Review

- This policy will be reviewed annually to ensure alignment with employment legislation and best practices.
- Employees with questions or concerns about maternity leave should consult HR for additional guidance.

M - 1.4 Parental Leave Policy

1. Purpose

Telecom Computer Inc. is committed to supporting employees who become parents by providing unpaid parental leave in accordance with Ontario's Employment Standards Act (ESA). This policy outlines the eligibility, duration, and rights of employees taking parental leave following the birth or adoption of a child.

2. Scope

This policy applies to all employees who have been employed by Telecom Computer Inc. for at least 13 weeks prior to the start of their parental leave. It applies to biological parents, adoptive parents, and those assuming parental responsibility for a child.

3. Parental Leave Entitlements

3.1 Duration of Leave

Eligible employees may take:

- 35 weeks of unpaid leave if they also took pregnancy leave.
- 37 weeks of unpaid leave for all other parents.

3.2 Timing of Leave

- For a birth mother who took pregnancy leave, parental leave must begin immediately after maternity leave, unless the child has not yet come into her custody, care, and control.
- For fathers and adoptive parents, parental leave must begin within 52 weeks after the birth or after the child first comes into the custody, care, and control of the parent.

4. Notice Requirements

- Employees must provide at least two weeks' written notice before starting their parental leave.
- If an employee does not specify an end date, it will be assumed that they will take the maximum allowable leave.
- If an employee stops working because the child arrives earlier than expected, they must provide written notice of their intent to take parental leave within two weeks of the child's arrival.
- Employees wishing to return earlier or later than originally planned (within the 35/37-week maximum) must provide at least four weeks' written notice of their new return date.

5. Benefits & Seniority During Leave

5.1 Benefits Continuation

- Employees on parental leave may continue participation in the company's benefit plan by covering both the employer and employee contributions.
- Payments must be made monthly, in advance, via cheque.
- If the employee fails to provide payment, benefits will be canceled immediately.

5.2 Seniority & Employment Rights

- Seniority will continue to accrue throughout the parental leave period.
- Employees on parental leave retain all rights to employment benefits, salary adjustments, and promotional opportunities upon their return.

6. Request & Approval Process

- Employees must submit a formal parental leave request to HR with the necessary documentation.
- HR will review requests to ensure compliance with ESA regulations.

7. Compliance & Policy Review

- This policy will be reviewed annually to ensure alignment with employment legislation and best practices.
- Employees with questions or concerns about parental leave should consult HR for additional guidance.

M - 1.5 Emergency Leave Policy

1. Purpose

Telecom Computer Inc. recognizes that employees may need to take time off to address urgent personal matters, illness, or family emergencies. This policy provides guidance on unpaid emergency leave in accordance with Ontario's Employment Standards Act (ESA) and ensures a consistent process for requesting and approving such leave.

2. Scope

This policy applies to all employees who may require emergency leave for unexpected situations, such as:

- Personal illness or injury
- Illness, injury, or medical emergency involving an immediate family member
- Other urgent personal matters that require the employee's immediate attention

3. Emergency Leave Entitlements

3.1 Unpaid Emergency Leave

- **E**mployees are entitled to up to 10 unpaid emergency leave days per calendar year.
- Emergency leave may be taken in full-day increments only—any leave taken for part of a day will be counted as a full day.

3.2 Relationship to Other Leaves

- Emergency leave is not an additional benefit beyond existing paid leave policies.
- Any bereavement leave, sick leave, or other company-provided paid leave taken will count toward the 10-day emergency leave allowance.

4. Request & Approval Process

- Employees must notify their supervisor as soon as possible when taking emergency leave.
- The company may require reasonable evidence (e.g., doctor's note, emergency documentation) to confirm that the leave was necessary.

5. Compliance & Policy Review

- This policy will be reviewed annually to ensure compliance with ESA regulations.
- Employees with questions regarding emergency leave eligibility should consult HR for clarification.

M - 1.6 Flexible Work Arrangements Policy

1. Purpose

Telecom Computer Inc. is committed to promoting work-life balance and enhancing employee productivity by offering flexible work arrangements where appropriate. This policy provides guidelines for employees seeking alternative work schedules, remote work opportunities, or modified duties to better accommodate their personal and professional needs.

2. Scope

This policy applies to all eligible full-time employees of Telecom Computer Inc. who have completed a minimum of one (1) year of continuous employment. Part-time and contract employees are not eligible for flexible work arrangements under this policy.

Eligible flexible work arrangements include:

- Remote Work (full-time or partial remote work)
- Flexible Scheduling (adjusted start/end times, compressed workweeks)
- Modified Duties (accommodations for health-related issues or other circumstances)

3. Eligibility

- Employees must have completed a minimum of one (1) year of continuous full-time employment to be eligible for flexible work arrangements.
- Eligibility is determined based on role requirements, departmental needs, and job performance.
- Requests for flexible work arrangements may be made to accommodate:
  - Health-related issues (e.g., disability accommodations).
  - Family responsibilities (e.g., childcare, eldercare).
  - Work-life balance preferences.

4. Types of Flexible Work Arrangements

4.1 Remote Work

- Employees may request to work from home or another off-site location.
- Remote work requires secure internet access, proper equipment, and adherence to company data protection policies.
- Remote work schedules must be pre-approved by management.

4.2 Flexible Scheduling

- Employees may request adjustments to their regular working hours.
- Options include:
  - Adjusted start/end times.
  - Compressed workweeks (e.g., working longer hours over fewer days).
  - Split shifts (working non-consecutive hours in a single day).
- Approval will depend on business needs and the employee’s ability to meet performance expectations.

4.3 Modified Duties

- Employees requiring temporary or permanent adjustments to their duties due to medical conditions or personal circumstances may request modifications.
- Accommodations will be made based on the employee’s abilities, role requirements, and business needs.
- Requests must be accompanied by medical documentation if applicable.

5. Request & Approval Process

- Employees must submit a Flexible Work Arrangement Request Form to their immediate supervisor or HR.
- The request must include:
  - The type of arrangement being requested.
  - The proposed work schedule or modifications.
  - The reason for the request.
  - The expected duration of the arrangement (if applicable).
- Supervisors will review requests based on operational requirements, employee performance, and job compatibility.
- Approved arrangements will be documented and signed by both the employee and the supervisor/manager.

6. Evaluation & Monitoring

- Approved flexible work arrangements will be evaluated periodically to ensure continued effectiveness.
- Adjustments may be made based on business needs or changes in the employee's performance.
- Supervisors may revoke or modify the arrangement if it no longer meets business or performance standards.

7. Compliance & Policy Review

- Violations of this policy or misuse of flexible work arrangements may result in disciplinary action, including termination.
- This policy will be reviewed annually to ensure alignment with business goals and employee needs.
- Employees are encouraged to provide feedback on the effectiveness of their flexible work arrangements.

M - 1.7 Paid Time Off (PTO) Policy

1. Purpose

The purpose of this policy is to provide employees with Paid Time Off (PTO) options, including Vacation, Statutory Holidays, and other approved time off. This policy outlines eligibility, procedures for requesting PTO, and expectations for usage.

2. Scope

This policy applies to all full-time, part-time, and contract employees of Telecom Computer Inc. unless specified otherwise. It governs:

- Vacation Time
- Statutory Holidays
- Carrying Forward Unused Vacation
- Termination and PTO Payout

3. Vacation Policy

3.1 Vacation Eligibility & Entitlement

- 1 to 5 Years of Continuous Service:
  - Paid 6% of gross pay as vacation pay.
  - Entitled to three weeks of vacation time.
- 5 to 15 Years of Continuous Service:
  - Paid 8% of gross pay as vacation pay.
  - Entitled to four weeks of vacation time.
- 15 or More Years of Continuous Service:
  - Paid 10% of gross pay as vacation pay.
  - Entitled to five weeks of vacation time.

3.2 Vacation Requests & Approval

- Vacation requests must be submitted in writing at least:
  - Seven (7) days in advance for single-day requests.
  - Fourteen (14) days in advance for requests of more than one day.
- Approval is based on business needs. Where two employees request the same period, the date of hire will be used as a tiebreaker.
- Employees are encouraged to take their full vacation allotment each year.

3.3 Carrying Forward Unused Vacation

- Unused vacation days may be carried forward to future years with Department Manager approval.
- Approval to carry unused days forward will be limited to the total annual vacation from the previous year.

3.4 Vacation Interruption Due to Statutory Holiday

- If a paid statutory holiday falls or is observed during an employee’s vacation period, an additional vacation day with pay will be provided at a mutually agreeable time.

3.5 Termination & PTO Payout

- Employees terminating employment are entitled to a proportionate payout of earned vacation pay up to the date of termination.

4. Statutory Holidays

4.1 Recognized Statutory Holidays

The following statutory holidays are recognized by Telecom Computer Inc.:

- New Year’s Day
- Family Day
- Good Friday
- Victoria Day
- Canada Day
- Labour Day
- Thanksgiving Day
- Christmas Day
- Boxing Day
- Civic Holiday (Not a statutory holiday)

4.2 Statutory Holiday Pay Eligibility & Calculation

- Employees who qualify for statutory holidays will receive regular earnings for the day (no shift premium).
- If a statutory holiday falls on a scheduled day off, an alternate day will be designated.
- To qualify for holiday pay, employees must have worked their scheduled shift before and after the holiday, unless there is a reasonable cause.

4.3 Working on a Statutory Holiday

- Employees scheduled to work on a statutory holiday will be paid:
  - 1.5 times the normal rate of pay for all hours worked.
  - An additional amount equal to one day’s regular earnings.

4.4 Holiday Pay Calculation

- Holiday pay is calculated as:
- The total amount of regular wages and vacation pay for the four weeks prior to the holiday, divided by 20.

4.5 Statutory Holidays During Vacation

- If a statutory holiday occurs during an employee’s vacation or scheduled day off, they will receive a day in lieu or a day's pay.

5. Compliance & Enforcement

- Employees are required to submit vacation requests within the designated timeframes.
- Misuse of PTO policies or unapproved absences may result in disciplinary action.
- Telecom Computer Inc. will periodically review this policy to ensure alignment with legal requirements and company objectives.

N - 1.1 Employee Volunteerism & DEI Advocacy Policy

1. Purpose

Telecom Computer Inc. encourages employees to actively participate in community engagement and diversity, equity, and inclusion (DEI) initiatives. This policy provides guidelines for volunteer opportunities, corporate-sponsored service projects, and DEI advocacy efforts, empowering employees to make a positive social impact while aligning with the company's values and mission.

2. Scope

This policy applies to all employees and covers volunteer activities, corporate philanthropy, DEI advocacy, and leadership participation in social impact initiatives.

3. Volunteerism & Community Engagement

3.1 Paid Volunteer Days

- Employees are eligible for up to two paid volunteer days per year to participate in their own community service efforts, environmental projects, or charitable initiatives.
- Volunteer activities must align with Telecom Computer Inc.'s CSR and DEI commitments.

3.2 Corporate-Sponsored Volunteer Programs

- Telecom Computer Inc. will organize annual volunteer opportunities such as:
  - Technology literacy workshops for underserved communities.
  - Environmental sustainability projects (e-waste recycling, tree planting, clean-up drives).
  - Indigenous community initiatives (mentorship programs, economic development support).

3.3 Employee-Initiated Volunteering

- Employees may propose volunteer projects that align with company values.
- HR will review and approve proposals based on impact, feasibility, and company priorities.

4. DEI Advocacy & Employee Engagement

4.1 Diversity & Inclusion Leadership

- Employees are encouraged to champion DEI initiatives by participating in:
  - DEI training, panels, and awareness campaigns.
  - Industry partnerships that promote diversity in technology.

4.2 Mentorship & DEI Programs

- The company will provide resources and training to support mentorship and advocacy efforts that align with Telecom Computer Inc.'s CSR and DEI commitments.

5. Request & Approval Process

- Employees must submit volunteer requests to HR at least two weeks in advance.
- Requests will be reviewed based on business needs and alignment with corporate values.
- Employees are responsible for ensuring that volunteer work does not interfere with core job responsibilities.

N - 1.2 Equal Pay & Pay Transparency Policy

1. Purpose

Telecom Computer Inc. is committed to pay equity, salary transparency, and fair compensation practices that ensure all employees receive equal pay for equal work, free from discrimination. As a Certified Living Wage Employer with the Ontario Living Wage Network, we recognize that paying a living wage is an investment in the long-term prosperity of our workforce and the broader economy. This policy establishes our commitment to fair and transparent pay practices, ensuring compliance with Ontario's Pay Equity Act, labor standards, and industry best practices.

2. Scope

This policy applies to all full-time, part-time, and contract employees at Telecom Computer Inc. and governs:

- Salary structures and compensation reviews
- Pay equity across all job levels
- Transparency in pay decisions and career progression
- Commitments as a Certified Living Wage Employer

3. Equal Pay & Fair Compensation Commitments

3.1 Living Wage Employer Commitment

As a Certified Living Wage Employer with the Ontario Living Wage Network, Telecom Computer Inc.:

- Pays all employees—both direct and contract workers—the established living wage for the region(s) in which we operate.
- Recognizes that a living wage is distinct from the minimum wage, as it reflects the actual cost of living in local communities.
- Supports a healthy, skilled, and dedicated workforce through ethical wage practices.
- Maintains certification with the Ontario Living Wage Network, ensuring that our wage commitments remain up to date.

3.2 Pay Equity & Non-Discrimination

- All employees performing substantially similar work will receive equal pay, regardless of gender, race, ethnicity, disability, or other protected characteristics.
- Compensation decisions must be based on experience, education, skills, and performance.
- Regular pay equity audits will be conducted to ensure fairness across all roles.

3.3 Pay Transparency & Open Communication

- Employees have the right to access salary ranges for their roles upon request.
- Salary structures will be clearly communicated through HR policies and career progression frameworks.
- Managers and HR personnel will receive training on fair compensation practices and non-discriminatory pay decisions.

3.4 Salary Adjustments & Reviews

- Compensation reviews will occur annually to address pay disparities and market adjustments.
- Employees who believe they are experiencing unfair pay discrepancies may raise concerns confidentially with HR.

4. Compliance & Enforcement

- Telecom Computer Inc. will comply with pay equity legislation, living wage certification standards, and labor laws to ensure fair compensation.
- Violations of this policy may result in corrective action, salary adjustments, or process improvements.

O - 1.1 Confidentiality & Data Protection Policy

1. Purpose

Telecom Computer Inc. is committed to protecting confidential company, employee, and customer information. This policy expands upon the existing Confidentiality and Release of Information Policy, ensuring compliance with data protection regulations, cybersecurity best practices, and ethical data handling standards.

2. Scope

This policy applies to all employees, contractors, and business partners with access to sensitive information, including personal data, financial records, proprietary business information, and customer data.

3. Confidentiality Commitments

- Employees must protect sensitive company and client data from unauthorized access, disclosure, or misuse.
- Confidential data must only be shared with authorized personnel for legitimate business purposes.
- Employees handling personal or customer data must comply with privacy laws, including PIPEDA (Personal Information Protection and Electronic Documents Act).
- Data encryption, password protection, and secure storage must be used for all confidential files.

4. Consequences for Breaches

- Violations of this policy may result in disciplinary action, termination, or legal consequences.
- Employees must immediately report any suspected data breaches to IT and Security teams.

O - 1.2 Artificial Intelligence (AI) Use & Security Policy

1. Purpose

Telecom Computer Inc. recognizes the growing role of Artificial Intelligence (AI) in enhancing business operations, decision-making, and efficiency. This policy establishes clear guidelines for the ethical, secure, and compliant use of AI tools and technologies, ensuring the protection of company data, intellectual property, and stakeholder trust.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who interact with AI tools, systems, or applications within Telecom Computer Inc. and its affiliates.
It covers:

- AI tools used for data analysis, decision-making, automation, and customer interaction.
- AI-driven software, platforms, and proprietary models used for business purposes.
- Third-party AI systems and applications used by Telecom Computer Inc. or its contractors.

3. Authorized Use

To mitigate risks and ensure compliance, employees must:

- Use only AI tools approved by the IT department, ensuring proper licensing and security standards.
- Obtain explicit authorization from management before using AI tools for processing sensitive company data.
- Verify AI-generated outputs for accuracy and reliability before relying on them for decision-making.
- Ensure AI applications align with Telecom Computer Inc.’s business objectives, security standards, and ethical guidelines.

4. Data Security & Confidentiality

- Employees must not input, upload, or share sensitive company data (e.g., customer information, financial records, proprietary information) with any AI tool unless explicitly authorized.
- Use of AI must comply with data protection regulations, including PIPEDA and applicable international standards (e.g., GDPR, CCPA) if relevant.
- All AI tools must be regularly updated and patched to prevent vulnerabilities and unauthorized access.

5. Prohibited Use of Public AI Models

Employees are strictly prohibited from entering, uploading, or sharing confidential, proprietary, or sensitive company or customer data into publicly available AI models, including:

- Free or open-source AI tools (e.g., ChatGPT, Google Bard, Claude, DALL·E, etc.).
- AI services where data inputs may be stored, analyzed, or reused by external parties.
- AI applications that do not meet Telecom Computer Inc.'s security and compliance standards.

Examples of sensitive data that must never be entered into public AI models include:

- Customer names, addresses, or personal information.
- Financial records, banking details, or pricing strategies.
- Proprietary business strategies, product roadmaps, or contracts.
- Employee or HR-related information.
- Any regulated or legally protected data under compliance frameworks (PIPEDA, GDPR, CCPA, etc.).

6. Access Control & Risk Management

- Access to AI tools must follow the principle of least privilege (PoLP), restricting usage to authorized personnel.
- Multi-factor authentication (MFA) and strong password policies must be applied to AI systems.
- AI-generated data and insights must be verified and reviewed by a human before implementation, especially in critical business functions.

7. Monitoring, Compliance & Auditing

- The IT and Compliance departments will monitor AI usage to ensure adherence to security policies and mitigate risks.
- Regular security audits and risk assessments will be conducted to identify vulnerabilities and enforce compliance.
- Employees must report any security incidents, AI biases, or data breaches involving AI tools immediately to the IT department.

8. AI Training & Awareness

- Employees must participate in mandatory AI training programs covering:
  - Data security & AI risk management.
  - Ethical AI principles (fairness, transparency, accountability).
  - Identifying AI-generated misinformation and biases.
- Employees are encouraged to stay informed about AI advancements and emerging threats.

9. Ethical Use of AI

- AI tools must be used responsibly and in alignment with ethical business practices.
- AI applications must not be used for discrimination, bias, or unethical decision-making.
- Employees must report any suspected unethical or harmful AI use to the Compliance team.

10. Data Privacy & Legal Compliance

- All AI-related data processing must comply with applicable data privacy laws (e.g., PIPEDA, GDPR, CCPA).
- Employees must ensure that AI usage respects individual privacy rights and maintains transparency in data collection and processing.
- AI models must follow data minimization principles, collecting only the necessary information for the intended purpose.

11. Enforcement & Disciplinary Action

- Violations of this policy may result in disciplinary action, including suspension, termination, or legal consequences.
- Telecom Computer Inc. reserves the right to restrict, audit, or revoke AI access if an individual violates security or compliance guidelines.

12. Policy Review & Updates

- This policy will be reviewed annually and updated to align with evolving AI regulations, technological advancements, and industry best practices.
- Changes to this policy will be formally documented and communicated to all employees.

O - 1.3 Email, Internet & IT Usage Policy

1. Purpose

Telecom Computer Inc. is committed to ensuring the secure, ethical, and responsible use of its email, internet, and IT resources. This policy establishes clear guidelines for acceptable usage, security practices, and compliance with legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to Telecom Computer Inc.'s:

- Email systems
- Internet access and web browsing
- Company-provided IT equipment and networks

3. Acceptable Use of Email & Internet

3.1 Business Use & Personal Use Limitations

- Company email and internet access must primarily be used for business purposes.
- Employees may use company internet for non-business activities only during meal breaks or outside of working hours, provided all other usage policies are adhered to.
- Internet usage must comply with corporate security policies and must not be used to engage in illegal, unethical, or inappropriate activities.

3.2 Prohibited Activities

Employees are strictly prohibited from:

- Displaying, storing, or distributing sexually explicit, offensive, or discriminatory material on company systems.
- Using company internet for illegal activities, including but not limited to software piracy, hacking, fraud, or unauthorized access to computer systems.
- Downloading, installing, or distributing unlicensed software or data that infringes copyrights or trademarks.
- Propagating malware, viruses, or any unauthorized software that could compromise company security.
- Disabling, overloading, or circumventing IT security systems that protect company assets.
- Engaging in online gaming, gambling, or entertainment streaming that is not directly related to job functions.

4. Email Usage & Confidentiality

- Employees must use their corporate email accounts responsibly and must not:
  - Send inappropriate, offensive, or misleading emails.
  - Transmit confidential company, customer, or employee information without authorization.
  - Use corporate email for personal business transactions or solicitation.
- Mass emails, video downloads, and large file transfers must be scheduled during off-peak hours to optimize network performance.

5. Social Media & Online Communication

5.1 Participation in Public Forums

- Employees must accurately represent themselves when engaging in online discussions, chat rooms, or newsgroups related to business activities.
- Employees may only speak on behalf of Telecom Computer Inc. if they are authorized representatives.
- Unauthorized employees must not endorse products or services on behalf of the company or engage in political advocacy under the company's name.

5.2 Confidentiality in Online Discussions

- Employees must never disclose confidential company information, trade secrets, customer data, or sensitive business strategies on any online platform, including:
  - Social media sites
  - Chat rooms
  - Public forums or newsgroups
- Employees who violate this policy may face disciplinary action, including termination.

6. Copyright & Intellectual Property Protection

- Employees must comply with copyright, trademark, and intellectual property laws when using internet resources.
- Software downloaded from the internet must be licensed and registered before use.
- Employees must not share or distribute copyrighted materials without explicit authorization.

7. IT Security & Access Control

7.1 User Authentication & Passwords

- Employees are responsible for maintaining the confidentiality of their login credentials.
- User IDs and passwords must not be shared with unauthorized individuals.
- Employees must follow multi-factor authentication (MFA) requirements where applicable.

7.2 Virus & Malware Protection

- All downloaded files must be scanned for viruses before being opened or executed.
- Employees must not disable or bypass company-installed antivirus or security software.

8. Monitoring & Compliance

- Telecom Computer Inc. reserves the right to monitor email, internet, and IT resource usage to ensure compliance with this policy.
- The company may block access to certain websites or services to prevent security risks and productivity loss.
- The company will comply with reasonable requests from law enforcement or regulatory agencies regarding employees' internet activity logs when legally required.

9. Consequences of Policy Violations

- Violations of this policy may result in disciplinary action, including termination.
- Employees found engaging in illegal or unethical activities using company IT resources will face legal action and potential criminal liability.

O - 1.4 Acceptable Use of Equipment Policy

1. Purpose

Telecom Computer Inc. provides employees with access to company-owned IT equipment, email, internet, and computing resources to support business operations. This policy outlines the acceptable and prohibited uses of company equipment to ensure security, compliance, and operational efficiency.

2. Scope

This policy applies to all employees, contractors, and authorized third parties using:

- Laptops, desktops, mobile devices, and network systems
- Printers, peripherals, and cloud-based applications
- Company email accounts and internet access

3. Acceptable Use of Company Equipment

- Company-owned equipment must be used for authorized business purposes.
- Limited personal use is allowed during breaks and non-working hours, provided it does not interfere with business operations.
- Employees must follow IT security protocols, including data encryption, antivirus protection, and software update compliance.
- Any use of company equipment must align with Telecom Computer Inc.'s policies on cybersecurity, confidentiality, and ethical business conduct.

4. Email, Internet, & Computer Use Policies

4.1 Email Usage Policy

- Company email accounts are provided for business use. Occasional personal use is permitted, but all messages are subject to company monitoring and access policies.
- Third parties (including suppliers, customers, or the public) are not permitted to use company email systems without prior authorization.
- Unauthorized access or "snooping" into another employee's email is strictly prohibited and will result in disciplinary action.
- The company may monitor email usage for security, compliance, and investigative purposes.
- Employees must not install unauthorized software or download executable files to company computers.

4.2 Internet Usage Policy

- The company reserves the right to monitor internet activity, including website visits, chat messages, emails, and file transfers. Employees should have no expectation of privacy regarding internet usage.
- Internet access must be used for business purposes, with limited personal use allowed during breaks.
- Employees must not visit, store, or distribute inappropriate content (e.g., sexually explicit, discriminatory, or illegal material).
- Downloading or sharing pirated software, copyrighted material, or malicious content is strictly prohibited.
- The company may block access to non-business-related websites to maintain network security and productivity.

5. Prohibited Use of Company Equipment

Employees must not:

- Use company devices for illegal, unethical, or unauthorized activities.
- Tamper with or disable security controls installed on company equipment.
- Connect unauthorized personal devices (e.g., USB drives, external hard drives) to company systems.
- Use company IT resources to engage in hacking, fraud, or unauthorized system access.
- Download or install unlicensed, pirated, or unauthorized software.

6. Security & Access Control

- Employees must lock company devices when unattended and report any lost or stolen equipment immediately.
- User IDs and passwords must be kept confidential and must not be shared with unauthorized personnel.
- Employees must use multi-factor authentication (MFA) where applicable.
- Any files downloaded onto company devices must be scanned for malware before being accessed.

7. Monitoring & Compliance

- Telecom Computer Inc. reserves the right to monitor and audit employee activity on company equipment, including email, internet usage, and file access.
- Violations of this policy may result in disciplinary action, including termination.
- The company will comply with lawful requests from regulatory agencies regarding employee IT usage logs when required.

O - 1.5 Cybersecurity & Threat Prevention Policy

1. Purpose

Telecom Computer Inc. is committed to protecting company systems, networks, and data from cyber threats, unauthorized access, and malicious attacks. This policy outlines proactive cybersecurity measures, employee responsibilities, and incident response protocols to prevent and mitigate cybersecurity risks.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party service providers with access to:

- Company networks, devices, and IT systems
- Cloud platforms, databases, and communication tools
- Sensitive business data, customer records, and proprietary information

3. Cybersecurity Responsibilities & User Guidelines

3.1 Employee Responsibilities

- Employees must comply with all IT security guidelines and report any security concerns to the IT department.
- All employees must use strong, unique passwords and enable multi-factor authentication (MFA) where applicable.
- Employees must complete annual cybersecurity awareness training to recognize and prevent cyber threats such as phishing, malware, and social engineering attacks.
- Any suspicious emails, unauthorized access attempts, or security breaches must be reported immediately to IT.

3.2 Acceptable Use & Secure Practices

- Company networks and devices must be used for authorized business purposes only.
- Employees must not connect unauthorized devices (e.g., USBs, external hard drives, personal laptops) to company systems.
- Downloading unapproved or unlicensed software is prohibited to prevent security vulnerabilities.
- Employees must lock their workstations when leaving their desks and secure mobile devices when working remotely.

4. Cyber Threat Prevention & Risk Management

4.1 Network Security & Endpoint Protection

- All company devices must have up-to-date security patches, antivirus, and endpoint detection software.
- Firewalls, intrusion detection systems (IDS), and secure email gateways must be configured to block malicious traffic.
- The IT department will conduct routine vulnerability assessments and penetration testing to identify and remediate security weaknesses.
- Unauthorized remote access or attempts to bypass company security controls will result in disciplinary action.

4.2 Email & Phishing Protection

- All company emails must be encrypted where applicable to prevent data interception.
- Employees must be vigilant against phishing emails that attempt to steal login credentials or install malware.
- IT will implement anti-phishing tools and conduct regular phishing simulations to improve employee awareness.

4.3 Data Loss Prevention (DLP) & Cloud Security

- Employees must store files in approved, secure cloud environments and avoid unauthorized external storage solutions.
- Sensitive customer and company data must not be shared or uploaded to public AI models or unapproved cloud platforms.
- IT will deploy data loss prevention (DLP) controls to monitor and prevent unauthorized data transfers.

.

5. Cyber Incident Response & Reporting

5.1 Incident Response Plan

If a cybersecurity incident occurs, the following steps must be taken:

- Identify the threat – Employees must report any suspected breaches, unauthorized access, or security vulnerabilities to IT immediately.
- Contain the breach – IT will isolate affected systems to prevent further damage.
- Investigate the impact – IT and compliance teams will assess which systems and data were affected.
- Mitigate the risk – Steps will be taken to remove malware, update security controls, and prevent recurrence.
- Communicate with stakeholders – If required, IT will notify affected employees, customers, or regulatory authorities.
- Post-incident review & policy update – IT will analyze the root cause of the incident and update security policies accordingly.

6. Compliance, Auditing & Enforcement

6.1 Security Monitoring & Audits

- IT will conduct regular cybersecurity audits to assess system vulnerabilities and policy adherence.
- Employees found violating security policies may face restricted system access, disciplinary action, or termination.
- IT reserves the right to monitor network activity and log security events to detect unauthorized actions.

6.2 Regulatory Compliance & Legal Obligations

- Telecom Computer Inc. complies with GDPR, PIPEDA, and other relevant cybersecurity regulations.
- Data protection policies will be updated as required to align with evolving cybersecurity laws

O - 1.6 Security & Access Control Policy

1. Purpose

To protect company assets, IT infrastructure, and sensitive information, Telecom Computer Inc. enforces a strict security and access control policy to prevent unauthorized access, data breaches, and physical security risks.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who require access to:

- Company buildings, restricted areas, and server rooms
- IT systems, networks, and confidential business information

3. Physical & Digital Access Control

3.1 Employee Access Management

- Employees must use authorized ID badges to access company premises.
- Unauthorized access to restricted areas is strictly prohibited.
- Employees must immediately report lost or stolen access cards to IT/security.

3.2 IT System & Network Access

- Access to company networks, cloud platforms, and IT systems is granted based on job responsibilities and the principle of least privilege (PoLP).
- Multi-factor authentication (MFA) is mandatory for all system logins.
- Employees must not share login credentials or access information with unauthorized personnel.

3.3 Security Audits & Monitoring

- Security logs will be reviewed regularly to identify unauthorized access attempts.
- Telecom Computer reserves the right to revoke access if an employee violates security policies.

4. Compliance & Enforcement

- Violations of this policy may result in access revocation, disciplinary action, or termination.
- IT and security teams will conduct periodic security audits to ensure compliance.

O - 1.7 Insider Trading & Ethical Financial Conduct Policy

1. Purpose

This policy ensures compliance with financial regulations and ethical business practices to prevent insider trading and conflicts of interest.

2. Scope

Applies to all employees, executives, and board members who have access to:

- Confidential company financial data
- Stock market-sensitive information
- Business strategies and internal performance reports

3. Insider Trading Regulations

- Employees must not trade company securities based on non-public information.
- Buying, selling, or recommending securities based on confidential company data is strictly prohibited.
- Employees must report any knowledge of insider trading violations to the President or Compliance Officer.

4. Ethical Financial Conduct Guidelines

- Financial reports and records must be accurately maintained in compliance with accounting standards.
- Employees must not engage in fraudulent financial practices such as misrepresentation, embezzlement, or falsification of records.
- Bribery, kickbacks, and financial misconduct are strictly prohibited.

5. Compliance & Enforcement

- Violations of this policy may result in legal prosecution, termination, or regulatory penalties.

Telecom Computer Inc. will cooperate with financial regulators and law enforcement in the event of a violation.

O - 1.8 Digital Records Management & Retention Policy

1. Purpose

To ensure compliance with legal, regulatory, and business requirements, Telecom Computer Inc. establishes secure and structured guidelines for data retention, storage, and disposal.

2. Scope

This policy applies to all employees, contractors, and third-party vendors handling:

- Financial records, employee files, customer contracts
- Email correspondence, cloud storage, and proprietary business data

3. Records Retention & Storage

- Company records must be retained for legally required periods before disposal.
- Sensitive data must be encrypted and securely stored to prevent unauthorized access.
- Employees must only use company-approved storage platforms for document retention.

3.1 Data Deletion & Disposal

- Records that are no longer required must be permanently deleted or securely shredded.
- Employees must not delete or alter financial, legal, or regulatory records without authorization.

4. Compliance & Auditing

- The IT and Compliance departments will conduct periodic audits to ensure proper record management.
- Failure to comply may result in disciplinary action or legal consequences.

O - 1.9 Third-Party & Vendor Security Policy

1. Purpose

This policy ensures that vendors, contractors, and third-party service providers meet Telecom Computer Inc.’s security, compliance, and ethical business standards.

2. Scope

Applies to all external vendors, IT service providers, and subcontractors handling:

- Company systems, infrastructure, and data
- Customer information, financial transactions, and procurement processes

3. Vendor Security Requirements

- Vendors must comply with Telecom Computer Inc.’s cybersecurity and data protection policies.
- Third-party access to company networks must be approved and monitored.
- Vendors must not store, process, or transfer company data outside authorized systems.
- Periodic vendor risk assessments and security audits will be conducted.

4. Compliance & Enforcement

- Non-compliance with security policies may result in contract termination and legal action.
- Vendors must report security incidents or breaches affecting company data immediately.

O - 1.10 Continuous Monitoring & Improvement Policy

1. Purpose

The purpose of this policy is to ensure the ongoing assessment, review, and enhancement of Telecom Computer Inc.'s cybersecurity, data protection, and financial integrity practices. By establishing a continuous monitoring and improvement framework, Telecom Computer Inc. aims to proactively identify vulnerabilities, mitigate risks, and ensure compliance with evolving regulations and industry standards.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and systems involved in:

- Cybersecurity & IT Infrastructure
- Data Protection & Privacy
- Financial Integrity & Recordkeeping
- AI Tools & Technology Usage

3. Continuous Monitoring & Improvement Requirements

3.1 Audits & Assessments

- Regularly conduct internal and external security audits to assess the effectiveness of cybersecurity and data protection systems.
- Perform vulnerability assessments and penetration testing to detect potential weaknesses.
- Evaluate financial reporting and data integrity procedures to ensure accuracy and compliance.

3.2 Policy & Procedure Updates

- Review and update policies to address:
  - Emerging cyber threats (e.g., malware, phishing, ransomware).
  - Regulatory changes (e.g., PIPEDA, GDPR, CCPA).
  - Technological advancements (e.g., AI systems, cloud security).
- Ensure that all employees are informed of policy changes and updated procedures through training sessions and official communications.

3.3 Incident Response & Remediation

- Continuously monitor for security breaches, data leaks, or unauthorized access attempts.
- Promptly address incidents through established incident response protocols.
- Conduct post-incident reviews to determine root causes and improve security measures.

3.4 Accountability & Reporting

- Designate IT, Compliance, and Financial Integrity teams to oversee monitoring and improvement processes.
- Ensure that incident reports, audit findings, and assessment results are properly documented and accessible for review.
- Regularly report findings to executive leadership and, when necessary, external stakeholders.

3.5 Culture of Continuous Improvement

- Promote a company-wide culture of continuous improvement and accountability.
- Encourage employees to report potential risks or security concerns without fear of retaliation.
- Foster an environment where best practices are regularly reviewed and enhanced.

4. Compliance & Enforcement

- Non-compliance with this policy may result in disciplinary action, including termination or legal consequences.
- Regular audits will ensure adherence to established protocols and identify areas for improvement.
- Management retains the authority to update this policy as necessary to align with industry standards and company goals.

5. Review & Updates

- This policy will be reviewed annually to ensure its effectiveness and alignment with technological, regulatory, and organizational changes.
- All changes will be formally documented and communicated to employees.