Trukumb Group ICT Policy

1 Introduction

The ICT policy for Trukumb Group outlines the guidelines and responsibilities for the use of Information and Communication Technology (ICT) across all its companies. This policy ensures the effective, secure, and ethical use of technology resources to support the business objectives of TruKumb Mining, Talen Vision Enterprises, Ivinar Park Academy, and Talen Vision Football Club.

Scope

This policy applies to all employees, contractors, and third-party service providers who use ICT resources of Trukumb Group. It covers hardware, software, networks, data, and communication devices.

Objectives

1. Ensure the efficient and effective use of ICT resources.
2. Protect the confidentiality, integrity, and availability of information.
3. Foster a secure and productive ICT environment.
4. Support the business goals of Trukumb Group.

2 Roles and Responsibilities

- **Business Transformation Department:** Oversees the implementation and compliance of the ICT policy.
- **Business transformation manager:** Manages day-to-day ICT operations, security, and support services.
- **Employees and Users:** Adhere to the ICT policy and report any breaches or issues.

3 Acceptable Use

- **Hardware and Software:** Users must use company-approved hardware and software. Unauthorized installations or modifications are prohibited.
- **Internet and Email:** Internet access and email use should be for business purposes. Personal use should be minimal and not interfere with work responsibilities.
- **Data Management:** Users must handle data responsibly, ensuring its accuracy and confidentiality.

4 Security

- **Access Control:** Access to ICT resources is based on user roles and responsibilities. Passwords must be strong, confidential, and changed regularly.
- **Network Security:** Firewalls, antivirus software, and encryption are to be used to protect the network from threats. Regular updates and patches are mandatory.
- **Data Protection:** Sensitive data must be encrypted. Regular backups should be conducted, and data recovery procedures must be in place.
- **Threat Monitoring:** Continuous monitoring for cybersecurity threats will be conducted. Anomaly detection systems will be in place to identify potential breaches.

5 Compliance and Monitoring

- **Policy Compliance:** Regular audits and reviews will be conducted to ensure compliance. Violations of the policy may result in disciplinary action.
- **Monitoring:** ICT use is subject to monitoring to ensure compliance and security. This includes internet usage, email communications, and access logs.

6 TRAINING AND AWARENESS

- **User Training:** Regular training sessions will be conducted to ensure users are aware of the ICT policy, security best practices, and any updates.
- **Awareness Programs:** Continuous awareness programs will be implemented to keep users informed about emerging threats and new ICT policies.

7 INCIDENT MANAGEMENT

- **Reporting Incidents:** Any ICT-related incidents, including security breaches, must be reported immediately to the Business transformation manager.
- **Incident Response:** A clear incident response plan must be in place to handle and mitigate the impact of ICT incidents.

8 ICT FOR EXTERNAL USERS

Access Management: External users will be granted access based on necessity and their roles. Access rights will be reviewed periodically to ensure they are up-to-date.

Confidentiality Agreements: All external users must sign confidentiality agreements before accessing Trukumb Group's ICT resources.

Monitoring: Activities of external users will be monitored to ensure compliance with the ICT policy.

Data Sharing: External users must follow strict guidelines for data sharing and handling. Any data exchanged must be encrypted and comply with data protection standards.

9 STAFF TRAINING AND AWARENESS

User Training: Regular training sessions will be conducted to ensure users are aware of the ICT policy, security best practices, and any updates. This includes phishing awareness, password management, and safe internet practices.

Awareness Programs: Continuous awareness programs will be implemented to keep users informed about emerging threats, new ICT policies, and cybersecurity trends.

External Users Training: External users will receive appropriate training to ensure they understand and comply with the ICT policy.

10 HARDWARE ANS SOFTWARE MAINTANACE

10.1 SECURITY UPDATES

1. **Importance:**
    - Security updates protect against vulnerabilities and threats.
    - Regular updates prevent unauthorized access, data breaches, and malware infections.
2. **Procedure:**
    - **Regular Schedule:** Security updates will be scheduled weekly or as needed based on the release of critical patches.
    - **Automated Updates:** Where possible, automated update systems will be used to ensure timely application of patches.
    - **Emergency Patches:** Critical updates must be applied immediately upon release. Systems may need to be temporarily taken offline to apply these patches.
3. **User Responsibilities:**
    - **Prompt Action:** Users must not delay the application of security updates and should allow automatic updates to proceed.

- **Reporting Issues:** Any issues encountered after security updates should be reported immediately to the ICT support team.

10.2 Hardware Upgrades

1. **Importance:**
    - Hardware upgrades enhance performance, extend the lifespan of devices, and support new software requirements.
2. **Procedure:**
    - **Assessment:** Regular assessments of current hardware performance and requirements.
    - **Approval:** All hardware upgrade requests must be approved by the Business Transformation Department.
    - **Installation:** Upgrades will be planned and executed with minimal disruption to operations, often scheduled during non-peak hours.
3. **User Responsibilities:**
    - **Cooperation:** Users must cooperate with the ICT support team during hardware upgrade processes.
    - **Careful Handling:** Users should handle upgraded hardware with care and follow usage guidelines to maintain its condition.

10.3 Software Updates

1. **Importance:**
    - Software updates fix bugs, introduce new features, and improve security.
2. **Procedure:**
    - **Regular Updates:** Routine checks and updates for all software applications.
    - **Version Control:** Maintain a record of software versions to ensure consistency across the organization.

- **Testing:** Updates are tested in a controlled environment before widespread deployment to avoid compatibility issues.

3. **User Responsibilities:**

   - **Timely Acceptance:** Users should not postpone software updates and should accept them as scheduled.

   - **Reporting Issues:** Any software issues encountered after updates should be promptly reported to the ICT support team.

10.4 Hardware Maintenance and Upkeep

1. **Importance:**

   - Regular maintenance extends the life of hardware and prevents unexpected failures.

2. **Procedure:**

   - **Routine Checks:** Periodic inspections and maintenance of all hardware components.

   - **Cleaning:** Regular cleaning of hardware to prevent dust and debris buildup, which can cause overheating and hardware failure.

   - **Repairs:** Prompt repair of any faulty hardware to prevent downtime.

3. **User Responsibilities:**

   - **Proper Use:** Users must follow provided guidelines for handling and using hardware to avoid unnecessary damage.

   - **Reporting Problems:** Any hardware issues should be reported immediately to the ICT support team for timely resolution.

   - **Regular Cleaning:** Users should keep their workspaces clean to prevent dust and debris from accumulating on hardware.

11 Guidelines on the Use of Cell Phones in the Workplace

11.1 Introduction

The use of cell phones in the workplace is an essential part of modern business communication. However, to maintain productivity, security, and a professional environment, Trukumb Group has established the following guidelines for the use of cell phones during work hours. These guidelines apply to all employees, contractors, and external users while on company premises or engaged in company business.

11.2 Acceptable Use

1. **Business Use:**
    - Cell phones may be used for business-related communications, including calls, messages, and emails, when required for work purposes.
    - Employees should ensure that their use of cell phones contributes to work efficiency and does not disrupt the work environment.
2. **Personal Use:**
    - Personal use of cell phones should be minimal during work hours and limited to breaks or emergencies.
    - Personal calls and messages should not interfere with the employee's duties or productivity.
3. **Use During Meetings:**
    - Cell phones should be set to silent mode or turned off during meetings, presentations, and other work-related gatherings unless their use is required for the meeting.
    - If urgent calls or messages are expected, employees should inform the meeting organizer in advance and excuse themselves discreetly if needed.

11.3 Security Considerations

1. **Confidentiality:**
    - Employees must be mindful of discussing sensitive or confidential company information over cell phones, especially in public or unsecured locations.
    - The use of company-provided secure communication apps is encouraged for business communications involving sensitive information.
2. **Device Security:**
    - Employees must ensure that their cell phones are secured with strong passwords, PINs, or biometric authentication to prevent unauthorized access.
    - Company-related data on cell phones should be encrypted, and regular backups should be performed.
3. **Company Wi-Fi and Networks:**
    - Employees should use secure connections, such as the company's Wi-Fi network, for accessing company emails, documents, or other resources.
    - The use of public or unsecured Wi-Fi networks for company business is discouraged unless protected by a virtual private network (VPN).

11.4 Prohibited Uses

1. **Inappropriate Content:**
    - Employees are prohibited from accessing, sharing, or storing inappropriate, offensive, or illegal content on their cell phones while at work.
    - This includes, but is not limited to, material that is discriminatory, harassing, or violates the company's code of conduct.
2. **Distractive Use:**

- Excessive use of cell phones for personal purposes, such as browsing social media, playing games, or streaming videos, during work hours is prohibited.
- Such behavior can result in disciplinary action if it affects work performance or disrupts the workplace.

11.5 Health and Safety

1. **Use in Hazardous Areas:**
   - Employees must adhere to safety regulations regarding cell phone use in hazardous or restricted areas, such as certain zones in TruKumb Mining.
   - In areas where cell phone use is restricted due to safety concerns, employees must follow all posted signs and instructions.
2. **Driving:**
   - Employees must comply with local laws and company policies regarding cell phone use while driving. Hands-free devices should be used if cell phone communication is necessary while driving on company business.

11.6 Enforcement and Compliance

1. **Monitoring:**
   - The company reserves the right to monitor the use of cell phones on company premises to ensure compliance with these guidelines.
   - Any misuse or breach of these guidelines will be subject to disciplinary action, up to and including termination of employment.
2. **Employee Responsibility:**
   - Employees are responsible for adhering to these guidelines and using their cell phones in a manner that upholds the company's values and operational efficiency.

- Any violations of these guidelines should be reported to the employee's supervisor or the Business transformation manager.

12 Guidelines on the Use of Social Media

12.1 Acceptable Use of Social Media

1. **Professional Use:**
   - Social media may be used to promote Trukumb Group's activities, engage with customers, and network with industry professionals.
   - Only authorized employees may post on official Trukumb Group social media accounts. These employees must ensure that content shared aligns with the company's branding, messaging, and values.
   - Employees are encouraged to share company achievements or updates on their personal social media profiles, provided the content is positive and accurate.
2. **Personal Use During Work Hours:**
   - Personal use of social media should be kept to a minimum during work hours and should not interfere with work responsibilities.
   - Accessing social media for personal reasons should be limited to breaks and should not disrupt the workplace or reduce productivity.

12.2 Content and Conduct Guidelines

1. **Confidentiality:**
   - Employees must not share confidential or proprietary information about Trukumb Group, its clients, or its partners on social media.
   - This includes but is not limited to financial data, business strategies, trade secrets, and personal information of colleagues or clients.
2. **Professionalism:**
   - Employees must maintain a professional tone when discussing Trukumb Group or work-related topics on social media.

- Negative comments or complaints about the company, colleagues, or clients should not be aired publicly. Such issues should be addressed internally through the appropriate channels.

3. **Respect and Non-Discrimination:**
    - Employees must not post content that is discriminatory, harassing, or offensive on social media, whether on personal or company accounts.
    - This includes content that could be seen as disrespectful or harmful to individuals based on race, gender, religion, sexual orientation, or any other protected characteristic.
4. **Brand Representation:**
    - When representing Trukumb Group on social media, employees must ensure that their profiles and posts reflect the company's values and uphold its reputation.
    - Employees should avoid engaging in arguments or disputes on social media that could reflect poorly on the company.

12.3 Legal and Ethical Considerations

1. **Intellectual Property:**
    - Employees must respect copyright and intellectual property laws when sharing content on social media. This includes not using or reposting copyrighted images, videos, or text without permission.
    - Employees should not use Trukumb Group's logos, trademarks, or other branding elements without authorization.
2. **Compliance with Laws:**
    - Social media use must comply with all relevant local, national, and international laws, including those related to privacy, data protection, and advertising.
    - Employees must avoid any activities that could lead to legal liability for themselves or the company.

12.4 Guidelines for Crisis Communication

1. **Crisis Response:**
    - In the event of a crisis (e.g., a negative incident involving the company), only designated spokespersons are permitted to communicate on social media.
    - Employees should refrain from posting about the crisis until an official statement is released by the company.
2. **Information Accuracy:**
    - During a crisis or otherwise, employees should avoid spreading unverified information that could mislead the public or cause unnecessary concern.

12.5 Enforcement and Compliance

1. **Monitoring:**
    - The company reserves the right to monitor employees' social media activities to ensure compliance with these guidelines, especially when using company equipment or accounts.
    - Any misuse of social media that violates this policy may result in disciplinary action, up to and including termination.
2. **Employee Responsibility:**
    - Employees are responsible for their conduct on social media, both in a personal and professional capacity, and must ensure their actions do not negatively impact Trukumb Group.
    - Any breaches of these guidelines should be reported to the employee's supervisor or the Business transformation manager.

13 Guidelines for Interaction About the Company on the Internet

13.1 General Guidelines for Online Interaction

1. **Accuracy and Truthfulness:**
   - Employees must ensure that any information they share about Trukumb Group is accurate, truthful, and up-to-date.
   - Speculation or sharing of unverified information about the company is strictly prohibited.
2. **Transparency:**
   - When discussing Trukumb Group online, employees must clearly identify themselves as company employees, particularly when engaging in conversations related to the company's business.
   - Employees should avoid anonymity when commenting on topics directly related to the company, as this can lead to a lack of accountability and potential misinformation.
3. **Respectful Communication:**
   - Employees should always communicate respectfully and professionally when discussing or responding to content about Trukumb Group.
   - Disagreements or negative comments should be handled tactfully, and employees should avoid engaging in arguments or hostile exchanges.

13.2 Confidentiality and Proprietary Information

1. **Protecting Company Information:**
   - Employees must not disclose confidential, proprietary, or sensitive information about Trukumb Group, its employees, clients, or partners.

- This includes internal discussions, business strategies, financial data, project details, and any other information not intended for public consumption.

2. **Social Media and Public Forums:**

   - Employees should be cautious when participating in public forums or social media platforms where information about Trukumb Group might be shared or discussed.

   - If an employee is unsure whether information is confidential, they should refrain from sharing it and consult with their supervisor or the Business transformation manager.

13.3 Endorsements and Testimonials

1. **Personal Endorsements:**

   - Employees should not provide endorsements or testimonials on behalf of Trukumb Group without prior authorization from the company.

   - Personal opinions expressed about the company or its products/services should be clearly stated as personal views, not official company statements.

2. **Use of Company Name and Branding:**

   - Employees must not use Trukumb Group's name, logo, or branding in a manner that implies endorsement or official representation without proper authorization.

   - Any use of company branding in personal online content should be approved by the relevant department.

13.4 Responding to Online Comments and Reviews

1. **Official Responses:**

   - Only authorized employees should respond to comments, reviews, or posts about Trukumb Group on the internet. These responses should reflect the company's official stance and messaging.

- Employees not authorized to speak on behalf of the company should refrain from responding to negative comments or reviews about Trukumb Group.

2. **Guidance for Non-Authorized Employees:**

   - Employees who come across negative or inaccurate information about the company online should report it to the appropriate department rather than responding directly.
   - If asked about the company online, employees should provide only basic, publicly available information and direct more specific inquiries to the appropriate company representatives.

13.5 Legal and Ethical Considerations

1. **Compliance with Legal Requirements:**

   - Employees must ensure that their online interactions comply with all applicable laws and regulations, including those related to defamation, privacy, and intellectual property.
   - Any statements made online that could expose Trukumb Group to legal risks are strictly prohibited.

2. **Avoiding Conflicts of Interest:**

   - Employees should avoid any online activities that could create a conflict of interest or give the appearance of bias when discussing or promoting Trukumb Group.
   - Employees must not engage in or endorse any activities online that could harm the company's reputation or financial interests.

13.6 Enforcement and Compliance

1. **Monitoring:**

   - Trukumb Group reserves the right to monitor online activities related to the company to ensure compliance with these guidelines.

- Any interactions that violate this policy may result in disciplinary action, up to and including termination of employment.

2. **Employee Responsibility:**

   - Employees are responsible for their online conduct and must ensure that their interactions about Trukumb Group are consistent with these guidelines.
   - Any potential breaches of these guidelines should be reported to the employee's supervisor or the Business transformation manager.

14 ICT Hardware and Software Requirements

14.1 Identification of ICT Hardware and Software Requirements

1. **Assessment of Needs:**

   - Conduct regular assessments of current ICT infrastructure to identify gaps, inefficiencies, and areas for improvement.
   - Collaborate with department heads and end-users to understand their specific needs and challenges.
   - Stay updated on emerging technologies and industry best practices to recommend appropriate solutions.

2. **Strategic Alignment:**

   - Ensure that the identified ICT requirements align with the overall business goals of Trukumb Group.
   - Prioritize requirements based on their potential impact on operational efficiency, security, and innovation.

3. **Documentation:**

   - Prepare detailed documentation of the identified hardware and software requirements, including specifications, expected benefits, and cost estimates.

- Develop a comprehensive business case for each requirement, highlighting the return on investment and alignment with strategic objectives.

14.2 Procedure for Procuring ICT Hardware and Software

1. **Submission to Finance Committee:**
   - Present the documented requirements and business cases to the Finance Committee for review.
   - Engage in discussions with the Finance Committee to justify the necessity and urgency of the proposed ICT investments.
2. **Approval or Adjustment:**
   - The Finance Committee will evaluate the submitted requirements and either approve, adjust, or reject the requests based on budgetary constraints and strategic priorities.
   - If adjustments are made, the Business Transformation Manager must revise the documentation and resubmit it for approval.
3. **Procurement Process:**
   - Once approved by the Finance Committee, the final list of ICT hardware and software requirements is forwarded to the Procurement Department.
   - The Procurement Department will follow standard procurement procedures, including vendor selection, quotation analysis, and contract negotiation.
   - The Business Transformation Manager may assist the Procurement Department by providing technical insights and ensuring that the selected vendors meet the specified requirements.

14.3 Roles and Responsibilities

- **Business Transformation Manager:**

  - Conducts assessments and collaborates with stakeholders to identify ICT needs.
  - Prepares detailed documentation and business cases for the identified requirements.
  - Presents and justifies the requirements to the Finance Committee.
  - Revises documentation based on feedback from the Finance Committee.
- **Finance Committee:**
  - Reviews and evaluates the submitted ICT requirements and business cases.
  - Approves, adjusts, or rejects the requests based on budget and strategic alignment.
  - Communicates the final decisions to the Business Transformation Manager.
- **Procurement Department:**
  - Manages the procurement process following the approval of the ICT requirements.
  - Engages in vendor selection, quotation analysis, and contract negotiation.
  - Ensures that procured ICT resources meet the specified requirements and are delivered in a timely manner.

15 POLICY REVIEW

This ICT policy will be reviewed annually or when significant changes occur in the ICT environment or business operations. Feedback from users will be considered during the review process.