ADD: P.O. BOX 3547
POLOKWANE, 0700
REG NO: 2009/004805/07
VAT NO: 451 018 0344

NATIONAL NUMBER: 0861 379 542 WWW.EPX.CO.ZA

Subject:	Electronic Communications Policy (HRP0006)
Compiled by:	CTL Group (Pty) Ltd
Authorised by:	Directors of E.P.X Courier Services
Implemented:	April 2021
Amended dates:	

Electronic Communications Policy:

(HRP0006)

1. INTRODUCTION:

1.1. This policy applies to all employees who have access to computers, various systems, and the Internet to be used in the performance of their work.

1.2. Employees not having access due to the nature of their jobs may not force or abuse another employee's access without permission. In such scenario, the perpetrator and the employee that had access may be disciplined.

1.3. Use of the Internet and internal electronic systems by employees is permitted and encouraged where such use supports the goals and objectives of the business. However, abuse in any shape or form will not be permitted and will result in disciplinary action. The terms and conditions of such will be addressed in this policy.

1.4. Employees may also be held personally liable for damages caused and/ or any costs involved by any violation of this policy.

1.5. This policy will ensure that all employees will have a clear guideline on what is permitted and what not.

1.6. In terms of Section 5 of the RICA Act (Act 70 of 2002), the law requires an employer to inform employees of such interception/monitoring and that such need to be governed under a policy within an organisation.

1.7. The Company's intention is to act in good faith by implementing this policy, in other words, serving a specific purpose to protect the company's interests and to ensure that any abuse in any shape or form be managed respectfully as per disciplinary code and procedure implemented.

2. POLICY:

2.1. Security Cameras:

2.1.1. As you are aware, cameras are installed at the security gates, in- and around the buildings & assets of the Company.

2.1.2. The purpose of the cameras is to protect the Company's property, employees, as well as customers visiting Company premises.

2.1.3. The footage is kept for an extensive period to be used as evidence if and whenever required for labour related matters and/ or criminal activity and the like.

2.1.4. The cameras are not deployed in inappropriate areas for example in restrooms/changerooms to protect individual's right of privacy.

2.1.5. The Company's focus is to create a safe working environment. Employees are therefore encouraged not to tamper with any camera as this will prevent the Company to protect you and or any other individual on company premises.

2.2. Biometric System:

2.2.1. This biometric system refers to the clock in system and fingerprint system gaining access to the Company's premises.

2.2.2. The purpose of this system is to keep track of attendance mainly and to be able to accurately submit information to the NBCRFI and or any external dispute resolution centre (CCMA) should the need arise.

2.2.3. Employees are required to clock in- and out every day. Employees will get paid accordingly.

2.2.4. No employee is permitted to clock in- or out for a fellow colleague or any other 3rd party without permission from management/supervisor.

2.2.5. This system also controls and further prevents any unwelcomed guests attempting to enter the Company's premises.

2.2.6. The Company further hired an external security Company controlling access at the main gates and accordingly must comply with this system criteria.

2.2.7. No clock in/out means absenteeism. In other words, "no work no pay" principle applies should there be no track of attendance record via the biometric system.

2.2.8. It is management instruction to employees to report for duty timeously, rather a bit early than late, to ensure that the correct arrival and exit times are recorded.

2.2.9. Employees are further advised to ensure proper communication between themselves and their superiors should there be any issues with the biometric system.

2.2.10. Any queries may be referred to in writing (via SMS/WhatsApp) to their superiors or HR for immediate intervention.

2.3. Licensed Software, Company E-mails, Computer/Laptops & devices:

2.3.1. Internal IT will ensure that all computers/ laptops and devices are approved and installed with “virus free” software.

2.3.2. No staff member is permitted to install any software or programmes without permission from IT.

2.3.3. Should a staff member utilize his/her own private devices or electronic equipment for business purposes, that IT has to be notified in writing and a check is required to be conducted prior using and/ or connecting the devices to the Company’s network.

2.3.4. IT is required to confirm on email that the device/equipment has been checked and permission was granted accordingly.

2.3.5. In case IT finds anything to be suspicious of nature or not granting permission, that the matter be escalated to Human Resources Department who will investigate and liaise with the required stakeholders for further instructions.

2.3.6. Employees are reminded that all Company Information remains confidential and that no 3rd party may be privy to private company information.

2.3.7. Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

2.3.8. All sites and downloads may be monitored and/or blocked by the Company, if they are deemed to be harmful and/or not productive to business.

2.3.9. Unacceptable use of the internet by employees includes, but is not limited to:

- Contact with adult phone lines or emails of a graphic, pornographic, adult, or political/religious content.
- The visiting of the site “Facebook” or related sites is strictly prohibited, however, whilst being on lunch employees are most welcome to access social media using their own data.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via the Company’s email service.
- Using computers to perpetrate any form of fraud, and/or software, film, or music piracy.
- Stealing, using, or disclosing someone else's password without authorization.
- Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization.
- Hacking into unauthorized websites.
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization

2.3.10. Should any employee at any given time not be sure whether certain company/client information may be shared or not that such employee will be required to approach HR for permission and/ or advise.

2.4. Internet / Wi-Fi:

2.4.1. Internal IT is responsible to ensure that all employees required to have access to Internet/Wi-Fi is indeed connected to be able to fulfill their work-related duties and responsibilities.

2.4.2. Employees may contact IT directly to ask for assistance during working hours pertaining any IT related query.

2.4.3. Usage will indeed be monitored by IT to prevent any form of abuse of Internet / Wi-Fi connection of which the Company is providing free of charge to the employee in good faith.

2.4.4. Any form of abuse or excessive cost implications due to any breach may be recovered from the employee(s) salary and this may result in further disciplinary action.

2.4.5. The Company reserves its right to either consult with the employee and/ or commence with disciplinary procedures.

2.5. Telephones & Company Cell phones:

2.5.1. This subject refers specifically to abuse of Company resources for private purposes.

2.5.2. The Company is indeed lenient to making quick private phone calls but that such calls be kept short, less than 5 minutes and not excessive in nature. Employees are then required to rather utilize their own private phones.

2.5.3. Phone records will be monitored randomly by the IT Department and any excessive usage shall be reported to the Department Head as well as to the Human Resources Department for further investigation and intervention.

2.5.4. The Company reserves its right to either consult with the employee and/ or commence with disciplinary procedures.

3. AGREEMENT:

3.1 It is confirmed that unless a formal objection thereto, is received in writing, it will be deemed that every employee, that has access to or has been supplied with any form of electronic communication device or equipment by the company, specifically agrees to the monitoring thereof.

3.2 I understand and will abide by this Internet Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.