1. **Revisions History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Modification Date** | **Purpose of the Modification** | **Section** | **Author** | **Approver** |
| 0.1 | 30/01/2020 | Creation |  | Pierre Bell | Pierre Augé BELL |

1. **Purpose of the document**

This document highlights the rules and customs to be followed any employee of Castel’s company part of the ICT Team and acting as and administrator in the information system of the company. Where some Administrative roles are also played by any third external consultant, this charter also applies to them and therefore they must be informed of the rules highlighted in this document.

The aim with this document is to protect the company Information system from illegal and damaging actions that could be performed by individuals either knowingly or unknowingly.

The purpose of this charter is to define who an administrator is, outline their roles, duties and responsibilities regarding their day to day interaction with the Information system.

These rules are in place to protect the company against cyberattacks, and data intrusions or stealing.

This document also acts as a guide for any newly hired administrator or as a refresher for any administrator who might require recalling the authorized and non-authorized in relation with interactions with IT items and systems under his responsibility.

Take note that the policy applies to all IT equipment owned or leased by the company

This document is part of the Security Management process of the ICT Management framework.

1. **Responsibilities**

Many actors are involved in this process:

* **Employee:** This group includes any individual officially contracted by Castel Malawi as a permanent or temporary worker
* **Contractor:** This group is constituted of all the companies and individuals contracted by CASTEL MALAWI to achieve specific jobs within the company sites but not part of the company’s Employees group.
* **Users:** Englobe all employees, Contractors, Consultant and any representation that could be a stakeholder in Castel’s operations
* **ICT Team Members:** This group includes any member of the ICT team, it could be a manager, a technician, an intern. They Ensure the execution of the process activities every day. They are responsible of:
* Checking the Systems
* Looking for threats
* Raise and sometimes mitigate the potential threats
* Prevent the threats by achieving the require preventive maintenance actions
* Update the protection databases repositories
* **ICT Managers:** this group includes the ICT Manager, the ICT Infrastructure&Helpdesk Manager, The ICT Business Manager and any other designated Manager in the ICT Organigram. They ensure the Process is followed by their team members, together they plan the Audits, they instruct the corrective actions, and they manage the ***Security Management controlling reports***.
* **Adminsitrator:** A member from the IT team or a partner of the IT department having advanced permissions on any system from the IS.

1. **Definitions:**

* **IS:** Information System
* **ICT:** information and Communication Technologies department of Castel malawi.
* **HOS (Head of Section):** Any Manager official in charge of one of the ICT sections.
* **HOD (Head of Department):** Any Manager officially heading a Department at Castel Malawi.

1. **Policy Description:** 
   1. **Context**

This Charter is intended for any person (hereinafter referred to as «Administrator») having, as part of his/her function or his/her professional activity and in an occasional or continuous manner, extended and privileged rights of access to the Information Systems Resources owned or made available at any of the Castel Malawi’s sites. These specific access rights allow him/her to ensure effective running of operations, to apply specific advance actions like patchings, changes, etc.. on part or whole IS.

These Administrators are responsible for the daily management of the company Information System Resources (such as servers, network equipment, security equipment, applications, databases, user workstations, etc.), and as such have privileged access rights.

The Administrator therefore has a key role which forces us in a security framework to ensure he is reliable. This will be done with couple of actions and implementation among which this charter which specifies the rules and precautions that each of them must comply with, in order to ensure a lawful, reliable and secure management of the Information Systems, while ensuring smooth running of operations.

* 1. **Missions:**

Administrators has a key role to play in the security ecosystem of the company; because of this, they must exercise, at all times, a reasonable degree of care, rigor and caution and self-awareness.

An Administrator missions are spread among activities like installation and configuration of hardware or software, the creation of access accounts, the allocation of rights or the setting up of backup means. He may also be required to show pedagogy towards Users whenever necessary to raise their awareness about the relevant rules for the use of Information Systems, good practices (including the professional use of electronic messaging, Internet and workstations) and procedures for handling security incidents. The Administrator shall ensure that all these rules are properly observed by Users.

In addition, some authorizations and privileged rights allow the Administrator to put in place monitoring and audit tools which may be useful or necessary to ensure the security of Information Systems against risks and misuse of the Information Systems Resources.

In particular, within the strict scope of his or her mission and the powers granted to him/her, the administrator may, in particular, be required to:

* Put in place means to audit the state of Information Systems and help provide technical information on network or applications administration.
* Conduct any technical verification of Information Systems Resources in order to detect any anomaly or incident that could hinder the proper functioning and security of the Information Systems;
* Take all the appropriate technical protection and / or correction measures to maintain and / or restore the security of the company Information Systems;
* Put in place and / or manage procedures, audits and statistical and / or ad hoc control tools meeting the requirements of security, proper use and sound operation of the Group's Information Systems, including the detection , analysis or filtering of all IT flows presenting a security risk (virus, intrusion, use of unauthorized software, etc.);
* Take all the appropriate technical measures in order to preserve evidence (logs, etc.) related to any anomaly, event or security incident or misuse of Information System Resources provided by the Company;
* Inform Users, by any appropriate means (letter, e-mail, internal note, etc.) of operations that may affect the proper functioning of the Information System (maintenance or upgrade operations, etc.);
* Take all the appropriate technical measures to effectively destroy data on equipment that is no longer in production or that has been reassigned;

As part of his/her missions, the Administrator may be required to access information for which he or she is not recipient, some information are confidential, private, or covered by the obligation of professional secrecy (secret - defense, etc.) and / or concerning the User activities. In this respect, he or she shall respect the confidentiality and sensitive nature of the information to which he may have access

In all cases, the Administrator must strictly comply with the applicable internal procedures establishing the framework and the scope of his or her intervention, as well as the hardware and software that he or she can put in place for that purpose.

* 1. **Duties:**

Administrators should use their access rights to the Information System Resources only when the exercise of their mission or functions requires it and not to access the desktop environment (electronic messaging, internet, etc.). Hence, the ownership of such privileged accounts is strictly intended for professional use.

The use of these non-nominative access rights must be prohibited and shall be made in accordance with the internal procedures authorizing it. Any action carried out on the Information shall be logged to ensure its accountability

Otherwise, the Administrators use their standard User account, without privilege, to access the Information Systems Resources made available by the Company.

In cases where the specific rules of this Charter do not apply. The Administrators must comply with the internal rules applicable to the Users of Information Systems.

Particularly given the overriding rights granted to the Administrator, this one should:

* Strictly act within the framework of his/her functions and should not abuse the privileged access rights granted to him or her. In addition, His or her action and access should not exceed the strict requirements of his or her mission and should be carried out in accordance with the procedures laid down for that purpose (the installation of unauthorized programs is prohibited , mechanisms for traceability must be deactivated, etc.);
* Strictly comply with the obligation of confidentiality and the applicable information confidentiality policies, by not disclosing professional information that would be brought to his/her attention in the course of his/her duties, In particular, He or she should refrain from copying any information or data collected via his or her access privileges, whose use exceeds the strict requirements of his or her functions or missions. Therefore, Any information on the organization, operation, management methods or even the urban plans of the Information Systems made available by the Company is considered confidential;
* Comply with all the security rules applicable within the Company (PSSI, etc.), by not bypassing established security procedures, unless compliance with applicable internal procedures requires it. In this regard, the use of information sharing software devices (FTP, P2P), the setting up of SSL tunnels, the use of software with listening or attack features or the use of virtual machines must be made in accordance with the conditions and circumstances indicated in the internal procedures which would provide for such acts;
* Verify the identification of any person who has authority to order him or her to take action on the Information Systems;
* Carry out preventive and curative maintenance on the Information System Resources made available by the Company, as well as file, data and processing backups required for the proper functioning of Information Systems and the continuity of the activities of all or part of the Company;
* Take part in all the logical and physical security audits and tests of Information Systems requiring it;
* Immediately inform his or her superior, the appropriate Information Systems Security manager and /or the persons authorized to intervene, of any event, security incident, detection of illegal content or activity or any violation of internal rules relating to the Information Systems resources made available by the company;
* Protect privileged accounts assigned to him/her and notify his or her superior, the appropriate Information Systems Security manager and /or the persons authorized to intervene, of any loss, theft, destruction or disclosure of his or her means of authentication. He or she shall in no circumstances allow the use of his or her privileged account by a third party;
* Contribute to the implementation of the most restrictive overriding access rights possible;
* If his or her missions require the granting of access rights to the Information Systems made available by the company(whether privileged accounts or not). Such granting can only be made on the parts of the Information System specifically covered by his or her scope of intervention. He shall also document the rights he grants and withdraw them as soon as they cease to be needed by the entrusted mission or, no later than the expiry date of the authorization validated by his or her hierarchy;
* If the access rights granted are privileged accounts. These rights must be granted according to the established procedures, by providing justifications for their implementation and by informing their holders that they are required to comply with this Charter;
* Promote and / or participate in all the measures aiming to protect the Company, including, participation in training and awareness-raising sessions on information systems security organized by the Company;
* Use the remote maintenance tools only in compliance with existing procedures;
* Follow up and document his or her actions in such a way that the Company has all the information necessary to pursue such missions during his or her absence or departure.

As part of his/her missions, the Administrator ensures that the Users properly use the Resources of the Information Systems made available by the Company and raises their awareness on good practices and applicable security rules.

It is recalled that Administrators performing control operations on the Information Systems are subject to the obligation of professional secrecy for the content featuring the keyword « [PRIV], belonging to the User's private life and which does not place in doubt the smooth technical operation of Information Systems, their security or the interests of the Company or those of any of the entities.

If this private information is transmitted to other departments of the Company. This transfer shall be made in accordance with the Group's applicable internal procedures and shall only involve the competent directorates or departments

* 1. **Control and Traceability:**

In accordance with the applicable internal rules and the legislation in force, The Company implements control procedures, which specifically include the recording and control of computer traces of all the actions carried out on the Information Systems it provides (the list of contents or services accessed, parameters for the management of hardware, data and software, authentication means, etc.).

Recordings, content and traces collected, as well as all the processing carried out, may be validly opposed by the Company or its technical service providers in order to prove any possible fault and sanction any failure.

For more details on the information collected and the implementation of control operations, see the « Company's Information System User Charter ».

* 1. **Compliance:**

The Administrator's attention is drawn to the fact that, besides adherence to the terms of this Charter, he or she shall also be required to comply with the legislative and regulatory provisions in force.

Non-compliance with the rules and measures set out in this Charter may entail the responsibility of the Administrator, and that of the service company for which he/she works if he/she is a partner. Account being taken, where appropriate, of the severity of impacts on the Company, He or she may be subject to disciplinary sanctions, or even legal or criminal proceedings in accordance with applicable law.

1. **Forms:**
2. **Attachments:**
3. **Related documents:**

ICT Charter

ICT Cyber Security Policy

1. **References:**
2. **Personal Commitment:**

I, the undersigned, ....................................................................... Declare that I have read and understood the « Administrator Charter»

Done in .................................................... on...................................

« Signature »