| Revision | Change Description |
|---|---|
| 00 | Initial Release |
| 01 | Revision after name change |

## Introduction

This document outlines the procedures to be followed by all Crown Paints Kenya PLC employees as far as ICT Systems are concerned and is referred to as the **ICT Systems User Access Policy**. It describes what steps need to be followed to allow users access company information systems. It also explains what procedures need to be followed from the time an employee joins the company up to the time of exit.

It is important that this document is read by all employees and adhered to at all times

## Need for ICT Systems Access Policy

All over the world, ICT systems are becoming the driving force behind most businesses. This means that most business processes today rely on the ICT infrastructure and Applications to run. In Crown Paints, the core business of manufacturing, distribution and sales of paints and related products heavily relies on ICT. ICT systems, helps manufacturing in maintaining all the product recipes and costs from inception of the company which act as a reference when modifying or making of the product. Similarly, selling and procurement of finished products and raw materials respectively together with the related financial and accounting procedures is made easier

Since accounting for such processes involves money, It is prudent that all users accessing information systems use the systems the way they were designed and not for individual selfish gains such as fraud. It is because of such gains that this policy has been designed and **MUST** be read, understood and signed by all employees who intend to access company ICT systems once employed. This signed document copy will be kept in the employee's file in the Human Resource Department. The employee shall be assigned user access passwords for the appropriate systems and any entries or transactions done on the ICT systems will be deemed to have been done by the person whose name appears against such transactions.

For this purpose, all users are asked to keep their passwords to themselves and not share them with other users or employees.

## Types of Employees

The employees will fall in two categories i.e. in contract and casuals. The contract employees include, fixed contracts and those with permanent terms of employment with the company. Casuals will consist of all employees with temporary terms of employment through a sub-contractor that provides manpower to Crown Paints and all employees on attachment/internship from the various colleges and universities.

## Access Policy Terms

- No one is allowed access to ICT information systems unless duly authorized by the management.

- All employees authorized to access ICT systems must be assigned a user code and password to access the systems. The user code will preferably contain one of the employee names or a number that uniquely identifies the employee.
- The authorized employees will be custodians of their passwords and shall be forced to change their passwords on the systems from time to time.
- All employees shall be responsible and answerable for transactions posted on the systems in their names or access codes.
- All authorized users must use their passwords to log onto the various systems and applications to transact business or generate documents. This will apply to all Office Applications as well.
- Access to ICT Data Centre's/Server Room will not be allowed to Non IT staff unless authorized by the head of ICT or his representative or the directors.

**The ICT Systems**

The ICT systems shall include the following:

**Hardware Infrastructure:** This consist of Data Center, Servers, Desktops, Laptops, IPad, Tabs, Printers and all the network infrastructure for access to LANs, WAN and Internet.

**Software:** This includes the Operating Systems and any application installed on it to enhance employee productivity e.g. Office, Enterprise Resource Planning System (SAP)

**Access to OS, Applications, Internet, Email and company ERP (SAP): Contract**

- On a new employee recruit to CPKL: The HR Manager/Assigned HR Officer will notify the IT Manager/Assigned ICT Officer by memo or e-mail.
- The head of Section/Depot/Department will complete a user access form (CPKPLC/ICTA: New Employee/Amendments) for the new user indicating which type of access the user needs based on the assigned duties and responsibilities and countersign the request form.
- The new user will carefully read this policy document, understand it and then countersign the form after which the same shall be forwarded to the ICT head for Approval.
- In the case of hardware i.e. Laptop, IPad, Tab the employee shall seek HOD and Financial Director or CEO approval.

- Once approved the head of ICT the rights shall delegate to the relevant ICT officer to grant permission to the system/relevant hardware purchased. The person granting the rights will countersign after the assignment of the rights has been done.
- The Access form shall be forwarded to the Human Resources Manager to be kept in the employee file.
- The access rights will be revoked on the user's leaving of employment. Such leaving will officially be communicated to the IT head by the Human Resource manager. This will be through a memo or email and by filling of form CPKPLC/ICT-C.
- In case a user access rights are to be changed, the form will have to be filled and countersigned afresh by the user and the head of section or department.
- Access to the Data Centers will be restricted to ICT staff or Authorized Employee only. In cases that Suppliers or vendors have to get to the data centers, they must be accompanied by at least one authorized ICT staff/ Authorized Employee.
- Employees must never share their passwords with anyone and shall be responsible for anything happening on the systems under their access accounts. All employees must adhere to the password policy assigned to the particular system being accessed.
- On an Employee leaving the organization or changing duties such that he or she does not need to access ICT systems, form (CPKPLC/ICT-C: Duty Alteration/Exit) shall be filled by the HR department and forwarded to the head of ICT for revocation of user rights. The form will be forwarded back to HR for filing once the sanction for change has been completed.

**Access to OS, Applications, Internet, Email and company ERP (SAP): Casuals**

- The rules above shall apply only that the Human Resource Manager should indicate on the form when such an employee will be leaving so that the ICT can disable/terminate the account when the employee leaves.
- Such employees should also have their records kept in a File within the HR Department. The records should include all details such as National Id, Place of Residence, Home and next of kin as well as referees and contacts.

**Employee Password Policy**

There is need to have a password policy. The policy ensures that users change their password regularly so that other people do not use them for their own personal gains. Because of this the following policy has been put in place and all users must follow it.

The following shall be the user password policy in Crown Paints:

Operating Systems (Windows/Linux/Android) and Crown Paints Domain.

1. Passwords must meet complexity requirements, that is
   - Contain Upper and Lower case characters ( E.g. Aa, Bb….Zz)
   - Contain at list a digit (E.g. 0, 1, 2,3 ….,9)
   - Be at least 9 Characters long (E.g. 2PackEpoxyEn or MyCatAte63Mice )
   - Be not more than 42 days old i.e. users must change the password after 42 days.
   - Password history must have 24 different passwords i.e. one cannot reuse the same password before he use nine other different passwords.
2. Passwords will be locked out after 5 attempts for a duration of 30 minutes. This means that after trying to log into windows five times, the user account will be blocked for 30 minutes unless ICT staff are called to intervene.

**SAP**

3. Passwords must meet complexity requirements, i.e.
   - Contain Upper and Lower case characters
   - Contain at list a digit and a non-alphanumeric - Be at least 8 Characters long
   - Be not more than 30 days old.
   - Password history must have 5 different passwords.

Passwords will be locked out after 3 attempts and the administrator must unlock the account after the 3 attempts for the user to access the system.

On a user leaving his workstation for 5 minutes unattended, the Windows Operating system and SAP will auto- lock. This can only be unlocked by the same user or the ICT systems administrator.

# CROWN PAINTS KENYA PLC

## CPKPLC/ICT-A: NEW EMPLOYEE / AMMENDMENTS

**ACCESS TO INFORMATION SYSTEMS REQUEST FORM**

Employee names as in the National Id /Passport /Work Permit

Mr. / Mrs. / Miss: _____

National Id /Passport No: _____ Signature_____

Expected Date of Exit (Casuals) _____

**I agree that I have read and understood the ICT Access policy document**

## DUTIES

| No. | Information Modules to be accessed / Equipment/ Functionality |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |

Immediate Superior :( Name, Signature &Date): _____

ICT Officer Granter Name & Sign: _____

ICT Effective Date: _____

ISO FORM FT-028-001 Rev/Issue: 00/01

# CROWN PAINTS KENYA PLC

## CPKPLC/ICT-C: DUTY ALTERATION / EXIT

**TERMINATION OF ACCESS TO INFORMATION SYSTEMS FORM**

**Employee Names as in the National Id /Passport /Work Permit**

Mr. / Mrs. / Miss: _____

National Id /Passport_____

The above named employee will not be required to access information systems with

Effect from (Date) _____

HR: Name & Sign (Must be signed if Employee is terminated):
_____

Immediate Superior: _____ Sign: _____

ICT access revoked by (IT): _____ Sign: _____

Date: _____

ISO FORM FT-028-002 Rev/Issue: 00/01

# CROWN PAINTS KENYA PLC

## CPKPLC/ICT-E: POLICY APPROVERS

Policy Effect (Date) _____

Policy Approver Name & Signature

Date: _____

**ICT MANAGER**

PATRICK MWATI
**FINANCE DIRECTOR**

Date: _____

RAKESH RAO
**GROUP CEO**

Date: _____

C.c Group CEO, Group Finance Director, All Department Heads, All Notice Boards