
# User Account Policy

Red Opal Innovations

Version 1

## Table of Contents

# Introduction

The purpose of this document is to outline the policies and procedures surrounding the creation, distribution and usage of computer user accounts within ROI.

# Authority to approve account requests

Approval to create accounts for new staff members is required from both the HR department and supervisor of the account holder. No accounts will be made without approval from a department manager and verification from HR that an Employment Contract has been signed.

User accounts can only be given to verified staff members of ROI. Visitors will not be given user accounts.

# Account creation process

Requests for new accounts need to be lodged via the Service Desk. This request must be initiated by the supervising manager of the account holder. Requests will be forwarded to the Network Manager for actioning, who will verify with HR that an employment contract has been signed. Due to the multiple parties involved in the process a lead-time of one week is required for all requests for new accounts.

For various reasons (such as Operating System upgrades, hard drive failures, etc.), the IT Department may need to delete and recreate your account. In an event such as this, and where possible, the IT Department will re-create the account to match the details of the old account.

# User accounts

All accounts will follow the naming convention below:

firstname.lastname

e.g. if your name was John Smith, your username would be:

john.smith

Where an existing user account already has the same username, middle initials will be used to differentiate the second account.

# Groups

Microsoft Windows utilises ‘groups’ to help collect user accounts together that have similar access privileges. ROI uses these groups to assign access to resources. When configuring access to a specific resource, the IT Department will assign groups access permissions to the resource. Individual user accounts, apart from the ROI-IT account (see below), will not be assigned access permissions. Users will gain access to a resource via the group they belong to.

Each PC in ROI will have the following standardised groups created on them. User accounts from each department will be added as members of their associated group, i.e. user accounts belonging to the staff working in the Multimedia Productions team will be members of the Multimedia group.

| Group Name | Department |
|---|---|
| IT-Dept | IT/Network |
| Development | Development |
| Multimedia | Multimedia Productions |
| Sales&Marketing | Sales and Marketing |
| HR | Human Resources |
| Accounts | Accounts |

## Access to resources

User accounts are provided to staff to gain access to the resources required to complete their work. Where a user account does not provide sufficient access to resources, requests to modify access must come from a supervising manager.

All staff accounts will be given 'Standard' access. Only IT accounts will be allowed to have 'Administrator' access. Guest accounts will be disabled.

## Account usage

Staff members must ensure that they use their own user account at all times. Account passwords cannot be shared or swapped, and logging in on behalf of another user is not permitted.

## Users' rights and responsibilities

It is a condition of employment that staff members must follow the ROI Acceptable internet usage policy provided at the commencement of employment.

## Disabling of accounts

Staff members who separate employment at ROI will have their user and email accounts disabled at 5pm on their last day. This is a security requirement as these resources can only be provided to ROI staff members.

## Password policy

Default passwords for new accounts will be set to the users' staff number provided by the Human Resources department. Users will be required to change this password the first time they logon.

When changing a password, all passwords are required to meet Microsoft complexity standards (minimum of six characters, with at least one numeral and one capital letter). Users will also be required to change their passwords every 120 days.

If a user account needs to be recreated, a password meeting the requirements in the paragraph will be created and forwarded directly to the account holder.

## Guest accounts

Guest accounts will be disabled on all computers.

## Administrator and IT accounts

Each PC is required to have an Administrator account that is used to control and configure the machine. Additionally, each PC will have the following account for use by the IT Department:

Username: ROI-IT

Both of these accounts can only be used by the IT Department.

## Recording of accounts

Each account will be recorded in a spreadsheet held by the IT Department. Data recorded will include the account holder's full name, manager, department, contact number, username, password, account type and PC the account is on.