GELOS
ENTERPRISES

User Account Policy

Contents

1. Introduction

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

2. User accounts

Each staff member is provided with a unique computer logon which is used to access the computers and email at Gelos. All accounts will follow the naming convention below:

firstname.lastname

For example, 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.

2.1 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 Gelos staff members.

2.2 Account creation process

Requests for new accounts need to be lodged via the ICT Systems Support Service Desk. This request must be initiated by the supervising manager of the account holder. Requests will be forwarded to the ICT Support Senior 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 ICT Systems Support team may need to delete and recreate your account. In an event such as this, the ICT Systems Support team will re-create the account to match the details of the old account (where possible).

2.3 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 ICT accounts will be allowed to have 'Administrator' access. Guest accounts will be disabled.

2.4 Account usage

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

2.5 Users' rights and responsibilities

It is a condition of employment that staff members must follow the Gelos Internet usage policy provided at the commencement of employment.

2.6 Guest accounts

Guest accounts will be disabled on all computers.

2.7 Disabling of accounts

Staff members who separate employment at Gelos 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 Gelos staff members.

2.8 Recording of accounts

Each account will be recorded in a database held by the ICT 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.

3. Groups

Microsoft Windows uses 'groups' to help collect together user accounts that have similar access privileges. Gelos uses these groups to assign access to resources. When configuring access to a specific resource, the ICT Systems Support team will assign groups access permissions to the resource. Individual user accounts, apart from the GE-ICT 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 Gelos will have the following standardised groups created on them. User accounts from each department will be added as members of their associated group, that is, user accounts belonging to the staff working in the Human Resources Department will be members of the HR group.

Group name	Department name
ICT	ICT
CustServ	Customer Service
HR	Human Resources
Finance	Finance
Marketing	Marketing
Ops	Operations
OCEO	Office of the CEO
Staff	All Gelos employees
Management	All Gelos managers
Project	Special projects team

4. Password policy

Default passwords for new accounts will be set to ‘Temp’ + the user’s staff number provided by the Human Resources Department (e.g. Temp131455). 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 eight characters
- Contains characters from three of the following categories:
    - Uppercase letters (A through Z)
    - Lowercase letters (A through Z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Users will also be required to change their passwords every 120 days.

If a user account needs to be recreated, a password meeting the required complexity standards will be created and forwarded directly to the account holder.

5. Administrator and ICT 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 ICT Department:

Username: GE-ICT

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

6. Version control

No	Effective	Approved by	Updates
1	20 August 20XX	Darren Cooper, Chief Technical Officer	Initial release