1. **Scope**
   1. This work instruction applies to the access to company systems.
   2. It must be read in conjunction with control section 9.2 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx), and all procedures identified there.
2. **Responsibilities**

The IT Manager is responsible for username administration.

1. **Work Instructions**
   1. Adding new users.

### For all new users there must first be a recently dated, fully completed and signed, original User Agreement. Users may only have one username, except as set out in the Adding New Administrators Section below. The account type and its individual requirements (group memberships, etc.) are decided by the CISO (DIRECTOR) against a role profile.

### A new user is allocated a username in line with the organisational naming convention. This is firstname.lastname@Retirement Capital.co.uk. There is no restriction on name length. This username is recorded on the User Agreement and, after the user account has been created (as set out below), the member of the IT Department creating the account signs and dates the User Agreement. A copy is retained in the IT Department file and the original is passed back to the HR Administrator.

### The IT Department maintains a log showing all user accounts, together with date of creation and dates of any changes and removal. This list is reviewed by the HR Administrator on a monthly basis to ensure that all usernames are still valid.

### Redundant usernames are never re-issued; all used usernames are held in the usernames record file and sorted to ensure that there is no duplication.

### Username: All lower case – [firstname.lastname@Retirement Capital.co.uk](mailto:firstname.lastname@x-tention.co.uk)

### Full Name: Full name of the user.

### Description: Enter title and base location

### Password: Random password generation*.*

## **Device provisioning (MAC-OS)**

* Reboot, holding down option key
  + Command R to enter recovery mode
  + Log in to WiFi
* Click on main disk name (top level)
  + Erase tab
  + Extended Journaled (NOT encrypted, NOT Case-sensitive)
  + [For older OS X versions] Name: APPLE SSD
  + Erase
  + Close
  + Set hard disk name as Macintosh HD
* Re-install OS X

Note that some of the options below may/may not apply to the version of OS X that was bundled with the device when it was manufactured

* Log in to WiFi (top-right) (don’t forget to allow access via mobile app)
* User account: “administrator” (1…)
* iCloud account: [administrator@Retirement Capital.co.uk](mailto:administrator@x-tention.co.uk)

We log in here so that the hard disk encryption key can be saved against this iCloud account

* + No 2FA
  + Do not upgrade
  + Disable stats, Siri etc.
  + No to keychain
  + No to register

### **Set Key Config Items**

* About my Mac
  + Software update
  + Enable “Automatically keep my Mac up to date”
* Keychain: later
* Filevault: Tick allow
  + Tick iCloud (so the recovery key is associated with the iCloud account)
  + Wait ~15 mins
* Send diagnostics: off
* Click clock (top-right) and set timezone
* App store
* Sign in
* Search “mojave”
* Install
  + (Computer wide) Settings
  + Users & Accounts
  + Disable Guest
  + Log in Options
  + Sharing
  + Computer name
  + <Asset ID> MacBook Pro
  + Security & Privacy
  + General
  + Require password: 5 mins
  + “Firewall” - “Turn On Firewall”
  + Screensaver
  + Flurry; 5 mins
* Open Chrome
  + Set as default

**Jump Cloud**

(After logging into the Mac as local admin)

* Ensure that the local admin user account has:
* “Account name”: “administrator”
* “Full name”: “Retirement Capital Administrator”
* Open Chrome and log in to XXX as an admin user
* “Systems” -> Add -> Download client
* Install client
* The system should then appear in XXX
* Set-up user in XXX
* Their username should be in the format forename.surname
* Ensure user has 2FA set-up in Google

### **Enable Google Admin Access**

* Install Chrome
  + Remove Safari from dock
* Open Chrome
  + Set as default browser <https://admin.google.com>
* Log in with my Google Account (an admin account)
  + Search “Endpoint verification” (<https://support.google.com/a/answer/9007320?hl=en> )
  + “Step 2 Add to Chrome”
  + Turn on sync
  + Don’t link password accounts
  + New button at top-right of Chrome
  + Agree
  + Add account
  + “Step 3 Download the native client”
  + Install as prompted
  + Click on icon on toolbar
  + “SYNC NOW”
* Restart Chrome <https://admin.google.com>
* Device management - device approvals
  + Right click on device
  + Approve
  + Company owned inventory
* Log out of Google account (top-right of Chrome)

## **Create User Account**

(Computer wide) Settings

* Users & Accounts
  + Create a user account

## Log in as user

## **Install Bitdefender**

A link to download Bitdefender has to be e-mailed from the Bitdefender log in area

If a user tries to re-install Bitdefender, it’ll say it found an installation and offers the user an uninstall option. However, they can’t do this as we’ve configured a Bitdefender policy to require a password [to uninstall the application]

## **Install Google Native Apps**

* Log in as user
* Google Drive <https://support.google.com/drive/answer/7329379>

If the installer shows an OS X window before the installer wizard window appears, then click Cancel (the installer wizard will then appear)

* Click logo appears at top-right of screen
* Restart browser
* Google Hangouts (chat/video) <https://tools.google.com/dlpage/hangoutplugin> )

## **Install Google Remote Desktop**

* Search “Google Remote Desktop”
* Want to download/install” the web version <https://remotedesktop.google.com/>
  + “Remote support” at top right
  + “Add to Chrome”
  + Install as prompted

## **Microsoft Office 365**

* Ring Zen Internet and ask for an additional licence to be added to the existing Microsoft Office 365 account. Provisioning takes up to 24 hours. Only Jon or Mark can do this (Zen won’t let anyone else access the account).
  + Log in to [www.office.com](http://www.office.com)
  + Create user
  + Use the built-in option to send the password to the user (choose the option to force the user to reset their password on next log in)
  + The user will receive the email
  + The user will log in with the Microsoft-created email address in the format forename.surname@XTentionLimited.onmicrosoft.com
  + Download Office (click “Install Office” at the top-right)
  + Install Office
  + Open an Office application (sign in with the forename.surname@XTentionLimited.onmicrosoft.com email address)
  + Don’t turn on Intelligent Services
  + Click “Continue to log in as” when the Google Drive Stream pop-up appears

## **Documentation**

## Complete Information Security Management System (ISMS) forms (ISMS-C-DOC-9.2.1a)

## **Vonage**

* Download and install desktop app

## **Asset Tag**

* Write out asset tag and affix to the back of the device
* Add to asset register spreadsheet (“Asset Register” document)

## **Password manager**

* Only use this to store access credentials for web sites
* Must not store access credentials for systems that have access to patient data

## **Encrypting USB Drives (VeraCrypt)**

(This doesn’t need doing as a matter of course, but some users may need it)

* Initially, erase the USB drive using “Disk Utilities”
* Need to download MacFUSE first (via a github.com link)
* Then download VeraCrypt
* Open VeraCrypt
  + Company policy is to encrypt the whole physical item
  + “Create a volume within a partition”

## **Points to Store Elsewhere**

Users must not delete or disable the “Administrator” account

***Document Owner and Approval***

The IT Manager is the owner of this document and is responsible for ensuring that this work instruction is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This work instruction was approved by the Managing Director on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |