

IT Security (HPC)

The primary method for accessing JCU HPC cluster servers is SSH (usually to `zodiac.hpc.jcu.edu.au`). On your first attempt to login you will be presented with fingerprint(s) for verification (security). If you don't see one of the following, contact HPC staff.

	MD5	SHA256	
ED25519	60:0f:e1:64:a7:2b:0e:ca:fa:26:fa:12:8f:14:d8:6e	JyjeD8XHZMJZPL68H4wzqUsQKZ+fwYFmng90fzLiA7A	
ECDSA	74:97:00:cb:7f:fc:3c:88:90:97:4f:4c:a3:4c:18:69	VCz2MjUcLCREVUJppsDZZigmQzvvjD2gFv7lw4oWuCY	
RSA	43:7d:80:97:51:15:d1:ff:82:e6:f2:6c:ca:59:1b:25	8EHGeEeDs jHTp2CPs8np8rKTgybXYPZ4FT3GN82dP5c	

Never give out your JCU central computing password to anyone. Avoid giving any other person to access your HPC account, if at all possible. If circumstances demand such access, it would be best to record the name of the person/people and the timeframe over which they had such access. It is also advisable that you watch and understand what they are doing.

Note: When it comes to incident investigations, you will be responsible for all actions associated with your account.

If you need or want to share your files/data with others, the following guidelines should be considered:

- For long-term sharing, submit a service-now request for creation of a group folder.
- All data in your HPC home directory will be archived (removed from HPC) after you leave JCU.
- Principle of least privilege
 - Ensure you have authority to share.
 - Share only what needs, and is safe, to be shared.
 - Submit a service-now request to create group(s) for sharing.
 - Sharing data as read-only incurs less risk than sharing read+write.
 - The more people you give access to, the more risk you incur. Anyone with write access to your files can overwrite/delete them accidentally (or deliberately).

JCU TS staff are working to turn off all desktop file shares (SMB protocol). Alternative options for researchers are:

1. Many national/international research areas already have mature facilities/services for housing, protecting, and/or publishing your research data. Ideally, these options should be your first choice.
2. AARNet CloudStor provides a storage option that can be seen by a greater spread of personal computing devices than HPC.
3. OneDrive provides up to 5TiB of storage to all JCU staff/students. Like CloudStor, this option is compatible with a very large range of personal computing devices.
4. Australian Research Data Commons (ARDC) will continue to provide resources for Australian researchers.
5. Several researchers and HPC staff are involved in a trial of Mountain Duck software as a replacement for traditional file shares (to personal computing devices). So far, all experiences have been positive, so this option is likely to be made available to anyone interested soon.
6. Public cloud resources are definitely a good option - control of usage becomes extremely important in this case.

Using JCU's VPN service is the safest way to access HPC resources when not on a JCU campus.

Currently, there is a JCU firewall exception that allows you to connect to HPC login nodes by SSH from off-campus - this exception may be removed in future.

HPC systems are automatically patched and scheduled reboots will occur. Generally speaking, HPC staff will try to avoid killing your jobs - but we may get directed to do work that will kill jobs/connections.

JCU HPC houses over 2PiB of research data. The price of backing up this amount of data is beyond our budget. Only use software from trusted sources.

If the software you are wanting to use isn't already available on HPC, submit a service-now request to have the software installed.

If you are developing software, ensure that the source code is held in a version control system (e.g., github or bitbucket).

Note: Many researchers choose to install software in personal directories. JCU TS security staff have identified significant risk to such privileges - HPC staff may be directed to configure a NOEXEC setting on HPC user filesystems in future. A sandpit-like environment will be made available for verifying safety of yet-to-be-trusted software if/when such a change is made.