جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

SHAHEEN
SUPERCOMPUTING LABORATORY

KAUST Supercomputing Laboratory HPC Systems

Terms & Conditions of Usage

07 March 2024

Prepared by:

Document Owner(s)
Maciej Olchowik, Systems Team, KAUST Supercomputing Laboratory

Version Control:

Version	Date	Author	Change Description
1.0	02 Oct 09	Richard Orme	Final Draft
1.1	30 Oct 09	Richard Orme	Revision 1
1.2	18 Jun 10	Richard Orme	Revision 2
1.3	18 Aug 10	Richard Orme	Revision 3
1.4	1 Mar 11	Richard Orme	Content & format update
1.5	3 May 11	Richard Orme	Included sample Acknowledgement statement
1.6	30 Jan 14	Andrew Winfer	Revision 6
1.7	12 Nov 15	Andrew Winfer	Removed references to BG/P
1.8	28 Feb 17	Andrew Winfer	Formatting and data policy
1.9	24 Jan 21	Andrew Winfer	Updated tier 4 countries
2.0	25 Sep 22	Maciej Olchowik	Updated for Shaheen3
2.1	28 Nov 22	Maciej Olchowik	Updated with organisations check
2.2	7 Mar 24	Maciej Olchowik	Updated links to forms (OAA, IAA, Project), added visiting staff info and OAA signatory policy, added links to the US consolidated screening list (CSL)

Section 1 - Export Regulations Compliance Requirements

1. The KAUST Supercomputing Laboratory (KSL) systems including, but not limited to Shaheen 3 and Ibex must only be used for student's education, and for scientific research, modelling and calculations in the following areas: solar energy, water desalination, clean combustion, catalysis, membranes, crops, composite and nanomaterials, Red Sea ecology, geosciences, modelling and visualisation, and computational genomics.
2. Access to the KSL systems at KAUST is only permitted to the following:
   a. Authorised students and faculty of KAUST (as certified by KAUST)
   b. Organisations and respective nationals of Tier 1, Tier 2 and Tier 3.
   c. Other organisations and institutions specifically approved by the US Government within the latest version of the Export License.
3. No access to the KSL systems at KAUST is authorised to organisations, governments or nationals listed on the US government consolidated screening list:

   https://www.trade.gov/data-visualization/csl-search
4. No use of the KSL systems at KAUST is authorised for any of the activities listed below:
   a. National security and/or intelligence work.
   b. The design, development, production, testing, or use of: conventional, nuclear, chemical, biological, or radiological weapons, or any component or subsystem specially designed for such devices.
   c. Complete rocket systems (including ballistic missiles, space launch vehicles, and sounding rockets) or unmanned air vehicle systems (including cruise missile systems, target drones, reconnaissance drones, and pilot optional aircraft) capable of delivering conventional, nuclear, chemical, biological or radiological weapons, including any specially designed component or subsystem of such systems.
   d. The design, development, production, use or maintenance of:
      i. A nuclear fuel cycle facility (including facilities engaged in nuclear propulsion and related activities) or heavy water production plant in a country not party to the Nuclear Non-Proliferation Treaty.
      ii. Any facility for the production of chemical, biological or radiological weapons.
      iii. Any facility for the manufacture of chemicals, biological agents or radioisotopes capable of being used in chemical, biological or radiological weapons.
5. Once granted, User IDs may NOT be used by anyone other than the person to whom that User ID was issued.
6. Business visitors at KAUST; as per University's policy; are considered as external users. OAA document will be required for such users (see section 2).
7. If user accounts are not used for more than 60 days, access to the KSL systems will be disabled and users will be required to apply to the KAUST Supercomputing Laboratory (KSL) System Administration (Sys Admin) Team via help@hpc.kaust.edu.sa for the account to be re-enabled.

Section 2 - Project Requirements

The ‘HPC systems and supporting services available through KSL are managed by the Research Computing Allocation Committee (RCAC) which was established by KAUST to manage KAUST’s research and training missions on the HPC systems. The HPC systems and services at KAUST are heavily utilised and KSL resources are allocated competitively.

Principal Investigators (PIs) are required to submit detailed proposals for their projects to obtain access to the HPC systems and services at KSL and will be required to report on progress relative to their approved proposal and work plan on a regular basis. Further, usage of the HPC systems and supporting services will be priced and charged in accordance with the policies dictated by the RCAC.

For non-KAUST users, their organisation or department must submit the Organisational Access Application (OAA), establishing a relationship between your home organisation and the KAUST Supercomputing Laboratory (KSL). The form should be completed, printed, signed, scanned and emailed to help@hpc.kaust.edu.sa. Each external organisation must have submitted a completed Organisation Access Application before its account requests or project proposals can be considered. The organisations should carefully consider who has the authority to sign the user’s applications for Shaheen Supercomputer on their behalf. This OAA application should be signed by the senior member of the management team. By signing this application, you acknowledge that you are responsible for updating the authorised signatory information upon any changes.

Project proposals must be submitted using form ‘KSL Project Proposal (PP) Template’. The form indicates elements which will be taken into consideration when assessing a project proposal for the allocation of resources and services, when reviewing project progress after it has been approved, and when analysing the costs of the project.

Project PIs are also required to submit progress reports on their project to KSL at least every 3 months. In addition to details of the project itself, these progress reports must, at minimum, include the following details:

- A description of all activities on the HPC systems since the previous report.
- Progress against the work schedule submitted with the Project Proposal.
- Expected completion date of the project.
- Any additional resources required to complete the project.

Note that projects will not be approved and set up without the organisation/institution having submitted an Organisational Access Application (OAA) and all users working on that project having submitted an Individual Access Application (IAA).

Users and organisations will be checked against the consolidated screening list published by the US government.

The OAA form is available for download at: http://hpc.kaust.edu.sa/

The IAA and Project proposal form can be completed online at http://apply.hpc.kaust.edu.sa

Section 3 – Data Purge Policies

- /scratch/<username> and /scratch/project/<projectname>: files not modified AND not accessed in the last 60 days will be deleted.
- /scratch/tmp: temporary folder - files not modified AND not accessed in the last 3 days will be deleted.
- /project/<projectname>: 20 TB limit per project. Once a project has used 20TB of disk storage, files will be automatically deleted from disk with a weighting based on date of last access. Stub files will remain on disk that link to the tape copy, so from a user's

perspective the file will still be visible on disk using normal commands such as ls, but will take take time to recover from tape back to disk if the file needs to be read.

- all data in /project/<projectname> and /scratch/project/<projectname> will be deleted permanently 1 month after core hour allocations for the project have expired unless a further application has been submitted for RCAC consideration.

Section 4 - Information Security Requirements

0.1 Introduction

Information Security (InfoSec) and Information Systems Management (ISM) policies are critical to KAUST's HPC activities, since the HPC facilities at KAUST represent a major component of KAUST's Information Technology infrastructure. InfoSec is the responsibility of every KAUST employee and any other individual or entity that uses the systems at KAUST. Users must ensure a high level of security in their use of KAUST Information Resources through appropriate behaviour, such as maintaining the confidentiality of passwords, and use of encryption tools for KAUST Classified Information. Users must never engage in any activity that would disrupt or compromise the availability, integrity, or security of KAUST information or the systems at KAUST, or otherwise result in their misuse. Users must immediately report all possible security breaches to KAUST management.

The Infosec and ISM policies applicable to the HPC facilities at KAUST are largely based upon the Infosec and ISM policies applicable to the whole of KAUST as determined by the CIO of KAUST.

0.2 Personal Privacy

a. Users should have no expectation of privacy concerning their use of systems at KAUST, including email, KAUST-provided computing equipment, the KAUST Intranet, KAUST-provided access to the public Internet, or other KAUST information systems. The required use of passwords to gain access to KAUST Information Resources is for KAUST's protection, and it does NOT imply that users can expect that their communications and use of the systems at KAUST are private.

b. By their use of these systems, and to the extent permitted by applicable law, users specifically consent to having their use and communications monitored and recorded. This consent only applies to the use of the systems at KAUST, and does not apply when a user obtains access to the public Internet outside of the KAUST computing environment or network (i.e. when access is not provided by KAUST) using their own personal computer.

c. Users are specifically advised that if possible illegal activity is detected, all information related to such activity, including text and images, may be provided to law enforcement authorities or third parties without prior notice to, or the consent of, users.

0.3 Potential Consequences for Violation of KAUST Policies

Failure to comply with KAUST policies may result in disciplinary or remedial action up to and including termination of a user's access to the HPC systems and other systems at KAUST and, when appropriate, termination of employment or other contractual relationship. Users may also be held responsible for damages to KAUST's IT systems caused by their violation of these policies.

1 - Workstation Security Requirements

1.1 Security of your Personal Workstation

The following security controls, if available, must be activated on all workstations to help protect against theft of sensitive KAUST information contained on the device:

- Activate a hard disk password for each drive in the device's BIOS settings.
- Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 30 minutes.
- Encrypt local databases, i.e. those residing on your workstation, that contain KAUST Confidential information, including mail files, archives, and database replicas.
- If you attach your workstation to a non-KAUST network where administrative level access on the workstation is not controlled by KAUST (e.g. you are working on an external organisation's network and are required to login to a Windows domain administered by that organisation), all KAUST Confidential information must be encrypted. Contact KAUST IT Security for recommended file/disk encryption solutions. Notes:

a. You are strongly advised to periodically change your workstation's hard disk password.
b. Desktop workstations located in Controlled Access Areas or in offices, which are locked when unattended, are not required to have keyboard/screen lock passwords applied.

1.2 When Leaving your Office or Work Area

If you do not work in an office that can be locked,

- Activate the password protected keyboard/screen lock when you leave, i.e., do not leave the workstation exposed for the 30-minute inactivity period required for the automated screen lock activation.
- If your laptop cannot otherwise be physically secured, i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken with you, a cable lock must be used to secure the laptop PC to a fixed object.

Notes:

a. Contact KAUST IT Security for recommended cable lock solutions.
b. If additional security controls are required, you will be notified by KAUST IT Security.

1.3 When Travelling or Working Away from your Office or Work Area

- Keep laptop PCs in your possession if at all possible.
- When travelling by air, do not put laptop PCs in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
- Laptop PCs should not be left for an extended period of time in an unoccupied vehicle. If you must leave your laptop PC in an unoccupied vehicle, then consider securing the laptop PC to the body of the vehicle inside the trunk. Information regarding how to best secure laptop PCs in a vehicle can be obtained from KAUST IT Security.
- If you must leave your laptop PC in a hotel, lock it in the hotel safe if one is available. If a safe is not available and you have a locking cable, use that mechanism.
- If you are travelling with KAUST Confidential material recorded on portable media

such as paper, diskettes, hand held devices (e.g. PDA, BlackBerry, mobile phone with data access, iPhone, etc.), laptop, etc., you must protect this media according to the same guidelines listed above for protecting your laptop PC.

Note: If your laptop, or KAUST Confidential information, is stolen or lost, you must immediately report the loss to KAUST IT Security, KAUST Security, and your manager.

1.4 Computer Viruses and Other Harmful Code

You must install and run a KAUST-approved antivirus program on your workstation. KAUST IT Security can advise you on what antivirus programs are considered acceptable.

Notes:

a. Antivirus clients should be configured to check for updated virus signatures at least daily.
b. If you discover a virus, advise KAUST IT Security.
c. If you are obligated to use an antivirus program not provided by KAUST, the antivirus program must meet the following basic criteria:
   - detect and block attempted actions by virus software in real time.
   - periodically scan for and detect virus software stored on the workstation.
   - check for virus signature control file updates on at least a daily basis.
   - must be a fully licensed product.
d. KAUST IT will only provide technical and Help Desk support for antivirus products provided by KAUST.

1.5 Firewalls

You must install and run a KAUST-approved client firewall program on your workstation.

Notes:

a. If you are obligated to use a client firewall product not provided by KAUST, the client firewall product must meet the following basic criteria:
   - detected networks should be treated as unknown and NOT trusted.
   - alert users to new programs requesting access to the network.
   - deny access from unauthorised systems.
   - the client firewall software must have the latest updates available.
   - must be a fully licensed product.
b. KAUST IT will only provide technical and Help Desk support for firewall products provided by KAUST.

1.6 File Sharing

You may allow other users to access or store files on your network-connected workstation only if the software that allows other users to access your files is provided by KAUST. This is to ensure that it has been adequately checked for security holes and legal and licensing restrictions.

Notes:

a. The use of Internet-based peer-to-peer file sharing services on workstations is prohibited unless explicitly approved by the KAUST CIO.
b. You must not allow anonymous FTP, TFTP, unauthenticated HTTP, or other unauthenticated access to areas of your hard disks that are also used for other purposes.

For example, you may not "share out" your entire hard drive with anonymous access.

c. You must not allow any form of unauthenticated access to data or programs that are classified KAUST Confidential, or to areas of your hard disk that may contain such data or programs.

d. If it is necessary to allow access to areas of your hard disk that are also used for other purposes (e.g. to allow remote maintenance or update of components of the operating system), or to KAUST Confidential materials, you must select either userid access control or password access control when defining the share options and the access must be granted only to the limited list of people with a need for that access, i.e. not to everyone who authenticates with a KAUST intranet password. Further assistance can be obtained from KAUST IT Security.

1.7 Workstation Operating System Currency

1.7.1 Major Service Releases

Personnel must install major service releases to their respective operating system version as soon as possible. The use of automated delivery solutions is recommended to simplify this requirement.

Users are encouraged to upgrade all local software themselves, but all upgrades to the centrally-managed KAUST HPC systems will be done by the KSL System Administrator (Sys Admin) Team, and must NOT be done by users without the explicit approval of the KSL Sys Admin Team.

1.7.2 Security Patches

Personnel must install security patches for their respective operating system version as soon as possible. The use of automated delivery solutions is recommended to simplify this requirement.

Users are encouraged to apply security patches to operating systems and other software on their local systems themselves, but all upgrades to the centrally-managed KAUST HPC systems will be done by the KSL Sys Admin Team, and must NOT be done by users without explicit written approval from the KSL Sys Admin Team.

1.8 Passwords

The password associated with a computer access userid is the primary means of verifying your identity, and subsequently allowing you access to the computer and to KAUST information. For your own protection, and for the protection of KAUST's resources, you must keep your identity verification password secret and not share it with anyone else.

KSL Sys Admin Team will use technical measures to enforce the password requirements.

Notes:

a. The hard disk password you use to help protect against unauthorised access to your workstation is not an identity verification password. This password is not associated with your identity, but rather can be managed like a door key or safe combination. It is not a violation of security policy for you to notify your manager of this password.

b. Information protection and data privacy laws in various countries include specific requirements for the selection of secure identity verification passwords, and compliance with these password rules is a legal obligation. The KAUST password rules listed below are consistent with current international requirements.

c. Identity verification passwords must not be trivial or predictable, and must:
   - Be at least 8 characters in length.
   - Contain a mix of alphabetic and non-alphabetic characters (numbers, punctuation or special characters) or a mix of at least two types of non-alphabetic characters.
   - Not contain your userid as part of the password.

d. Some KAUST systems and applications containing KAUST Confidential information require you to change your password at least once every three months (90 days). In cases where the system or application does not use technical control measures to force you to change your password, it is your responsibility to comply with this password change requirement. When changing your password, you must select a new password, i.e. do not change the password to one that you used within the past two years. You must not change your password multiple times in one day in order to re-establish a previously used password.

e. If you access computer systems that are not under KAUST control, do not select the same password for external systems that you selected for use on KAUST internal systems.

2 - Confidential Information & Intellectual Property (IP) Requirements

2.1 Copyright and Intellectual Property

Most information and software (programs, audio, video, data files, etc.) that is publicly available (including that on the Internet) is subject to copyright or other intellectual property right protection. When obtaining material for use on the KAUST HPC systems:

- Do not obtain software from such sources for use on KAUST HPC systems unless express permission to do so is stated by the material owner and the KSL Sys Admin Team.
- All software for use on the KAUST HPC systems must be installed by the KSL Sys Admin Team. If you require any software that is not already installed on the HPC systems at KAUST, you must place a request for that software with the KSL Sys Admin Team. The KSL Sys Admin Team will examine any applicable software copyright restrictions and discuss any issues with the requestor prior to the software being installed on the HPC systems. If the KSL Sys Admin Team believes that KAUST will not be able to comply with any part of the terms and conditions of use then that software will not be installed on the HPC systems at KAUST.
- Ensure that you comply with any expressed requirements or limitations attached to the use of such software, e.g. not to be used for commercial purposes; cannot charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy; must distribute source code; etc.
- If you are unsure about the meaning of the restrictive language or have questions about it, you should contact the KSL Sys Admin Team and KAUST Legal before using the material.
- You must obtain assistance and approval from KAUST Legal before incorporating any material that is not KAUST property into a product or material that KAUST intends to distribute externally.

2.2 Publishing KAUST Software

Seek advice from KAUST Legal before uploading any KAUST software to the Internet.

You must ensure that any KAUST copyright documents clearly indicate KAUST as holder of the copyright.

2.3 Residual Information

In situations where a KAUST or contract employee is using a PC owned by an organisation other than KAUST, the management owner of the equipment will retrieve KAUST data from specified workstations and inspect designated machines, upon request from KAUST. Contractor and non-KAUST management must take necessary actions to protect KAUST Confidential information.

All KAUST data and applications including access information and passwords must be deleted from workstations not provided by KAUST when there is no longer a legitimate need and authorisation for access.

2.4 Liability

In situations where non-KAUST assets are being used for KAUST business, KAUST is released of all liability in the event of loss/damage to the equipment and/or information. In cases where a non-KAUST workstation is used as part of a contractual relationship, appropriate releases must be signed as part of the agreement between KAUST and the contracted organisation or company.

2.5 Protecting KAUST Confidential information

The primary requirement for protecting KAUST Confidential information is that it must be protected from access or viewing by people who do not have a need to know the information.

KAUST Confidential information must be properly labelled '***KAUST Confidential***' in the header and footer of each page of the document.

KAUST Confidential information related to unannounced technology or business plans, non-public financial information, and personal information (e.g. credit card numbers, financial or medical information, etc.), must be encrypted if sent electronically across the Internet. Contact KAUST IT Security if assistance is required with encryption.

When you store KAUST Confidential information on computer systems (e.g. group web sites, or shared data repositories), you must use software security controls to manage and limit access to the information. Security controls must never be set to allow unrestricted (e.g., 'world-readable', "public") access to KAUST Confidential information. Security controls must control not only access to the data itself, but also User IDs which have access to the data. If you do not understand how to correctly set or use the security controls, you should ask for assistance from KAUST IT Security.

When you store KAUST Confidential information on removable computer media, such as diskettes, tapes, compact disks (DVDs/CDs), handheld device storage, etc., you must protect the information against theft and unauthorised access. Label the media '*KAUST Confidential*' and keep it in a locked area or storage device when not in use. Never leave removable computer media exposed in unattended areas.

Sensitive Personal Information (SPI) about KAUST's employees, our partners, or other individuals is to be classified KAUST Confidential.

a. Do not store SPI without a valid need to do so.
b. If you have a valid need to store SPI on your workstation or portable removable media (such as a CD/DVD, a removable HDD, a USB storage device, or a data backup tape), the information must be encrypted at the data, file or media level.
c. Refer to KAUST IT Security for approved cryptographic methods when storing SPI

locally on your workstation, and when storing SPI on portable removable media or other network attached backup destinations.

d. If your workstation or portable media containing SPI is lost or stolen, or if you suspect that somebody has compromised its security, you must immediately report the incident to KAUST IT Security and your manager, and specify what SPI may have been exposed. Follow the instructions provided in Section 4 - Security Incident Reporting below.

Do not enter KAUST Confidential information on Internet web sites that offer translation services, e.g. world.altavista.com.

When printing KAUST Confidential information, you must protect the information against theft and unauthorised viewing. In this context, the term ‘printer’ includes printers, plotters, and any other device used to create hard copy output.

KAUST Confidential information may only be printed:

- in a controlled access area, with access based on ‘need to know’, or
- in an attended KAUST printer facility, where the output is given only to its owner, or
- on a printer with capture/release facility that you control, or
- on a printer that you are personally attending.

If none of these options are available at your location, you may use a printer located within an open area in KAUST internal office space, but you must pick up your KAUST Confidential printout material within 5 minutes.

2.6 KAUST Internal Networks

When connected to and using KAUST internal networks, including Local Area Networks (LANs):

- Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
- Do not monitor network traffic (i.e., use a "sniffer" or similar device) without first obtaining explicit approval from the KAUST IT Network Administrators.
- Do not run security testing tools/programs against any Intranet system or server, other than those that you directly control, without first obtaining explicit approval from the KAUST IT Network Administrators.
- Do not add any network device that extends the KAUST infrastructure (e.g. devices or devices functioning as switches, bridges, routers, hubs, modems, wireless access points, etc. for any reason without first obtaining permission from the KAUST IT Network Administrators.
- Configure workstation wireless network adapters such that the workstation will only connect to the KAUST WLAN infrastructure, or to ‘safe’ wireless networks such as your secure home network. Workstations within isolated lab networks are prohibited from simultaneously connecting to the KAUST wireless LAN infrastructure and the isolated lab networks.

2.7 Computer Conferencing

KAUST internal computer conferencing (Newsgroups, Forums, Discussion Databases) provide KAUST-wide databases for sharing information and discussing ideas about a wide range of topics, as approved by the conference owners. Information and discussions on KAUST internal conferences must meet the following criteria:

- If the conference is set up to allow open participation within KAUST, or to allow participation by KAUST partners or other external parties, KAUST Confidential information must not be included or discussed.
- Non-technical information and comments which are more appropriate for an official KAUST communications channel (e.g., speaking to one's manager, etc.) must not be included.
- Participants must avoid giving legal opinions or medical advice.
- Secure computer conferencing services must be used when KAUST Confidential, personal or sensitive information is discussed.

2.8 Remote Connections to KAUST Networks and Systems

When connected to a non-KAUST network, a KAUST-approved remote access solution must be used to establish connectivity with KAUST. Contact KAUST IT Security for information on approved remote access solutions.

2.9 Using Public Systems

Public systems are not owned or controlled by KAUST and therefore are not subject to compliance with KAUST IT Security Standards. Examples of public systems are those which are provided at ‘hot spots’ and cyber cafés. Therefore, KAUST information is not to be stored or copied to the local file store on any public system, nor is access to KAUST internal resources allowed from public systems. KAUST internal resources, such as your email, should only be accessed from systems that comply with KAUST IT Security Standards.

***Notes*:**

a. It is acceptable to attach your laptop to the Internet connectivity at a ‘hot spot’ (e.g. cyber café, hotel, etc.) provided you are using a KAUST-approved remote access solution to establish connectivity to KAUST's internal infrastructure.
b. Though storage space that is provided to an individual by their Internet Service Provider (ISP) is not necessarily considered a public system, it is also prohibited to store KAUST information in an ISP's storage space.

3 – Acknowledgement of KAUST in Research Publications

Whenever the results of research conducted on the HPC systems at KAUST are published, or the research involved personnel from KAUST Supercomputing Laboratory (KSL), Principal Investigators (PIs) are required to acknowledge the usage of the HPC systems at KAUST and/or the involvement of KSL personnel in their research in their publications. For example, the following statement could be used: “*For computer time, this research used the resources of the Supercomputing Laboratory at King Abdullah University of Science & Technology (KAUST) in Thuwal, Saudi Arabia*.”

4 - Acceptable Usage

The following applies to all KAUST IT and HPC system users:

4.1 Maintain Professional Demeanour in Communications

Users must maintain a professional demeanour in all internal and external KAUST communications. Due to the nature of the computing environment, users must be mindful of the possibility that others may regard their communications as authorised or official communications of the company.

4.2 Avoid Inappropriate and Offensive Content

Users must never use KAUST systems to create, access, transmit or store any material that would be considered in bad taste, or otherwise inappropriate, offensive or disrespectful of others (e.g., obscene, lewd, pornographic or violent material, depicted nudity, sexually oriented jokes or cartoons, and/or other offensive material related to age, race, colour, sex, religion, national origin, disability or sexual orientation). Users encountering or receiving this kind of material should immediately report the incident to KAUST management.

4.3 Personal Use of KAUST Information Resources

a. Occasional, limited personal use of KAUST Information Resources is permitted if it is reasonable, ethical, and does not interfere with work responsibilities or conflict with local management directives. In general, personal use of KAUST Information Resources is not appropriate when it interferes with a user's overall productivity or performance on the job, is in conflict with the KAUST Security Policy or other policies and guidelines for employee conduct, places a burden on KAUST computing and communication resources, or otherwise hinders or prevents KAUST from conducting its business.
b. Use for Personal Political Activity or Personal Gain is prohibited.
c. KAUST Information Resources must never be used for personal political activity or personal profit or gain.

5 - Security Incident Reporting

A security incident can originate inside or outside of KAUST, can involve other KAUST internal or external sites, and can range in severity.

Incidents involving violations of KAUST policies can be referred to management or HR for resolution, including disciplinary action if needed.

If any security incident involves matters such as unauthorised access to classified or otherwise sensitive data (such as information about research or employees), alteration or compromising the integrity of a system/server/application, disruption or denial of service availability, alteration or defacement of an Internet website, system penetrations, destruction of data, fraud, crime, etc., you must adhere to KAUST IT Security's Security Incidents Guidelines for reporting the incident.

Note: KAUST personnel are NOT to attempt to investigate or take action against the offender unless directed to do so by KAUST IT Security personnel. KAUST IT Security staff are qualified and trained to properly contain exposures, mitigate potential impact to KAUST, and conduct investigations, up to and including gathering evidence for possible legal action.

If you have questions relating to security, discuss them with your manager or KAUST IT Security.