CHRIST (DEEMED TO BE UNIVERSITY)

OFFICE OF INFORMATION TECHNOLOGY (OIT)

Code of Conduct for IT Professionals

The Information Technology Resources of the University form the integral support structure for the University for Effective Conduct of its operational and administrative activities. In this context the accountability and responsibility of the Office of Information Technology (OIT) is of immense significance. Every employee of the University attached to the OIT has to be committed to the task he/she is entrusted with and has to carry out the same with utmost integrity and professionalism. In the course of their work requirements, they may access various data in applications, emails and file systems or on desktops, servers and networks and other systems which are critical assets of the University that must remain protected at all times. This Code of Conduct made in pursuance of the University Regulation for IT shall be applicable for all IT Professionals engaged by the Office of Information Technology (OIT) whether as employees of the University or through its Contractors and irrespective of the position or title they may hold.

1. The Technicians, Engineers (Software and Hardware), Technical and other Staff in Administration and Supervision (by whatever designation/title called) collectively referred to herein as IT Professionals, while being responsible for the IT Resources for the University must follow and bind themselves to Professional Ethics and Code of Conduct as provided herein, more specifically, the IT Professionals shall:
   a) Act consistently and as appropriate accept full responsibility for their own work.
   b) Approve software only if it is safe, meets specifications, passes appropriate tests, and does not diminish privacy or harm the environment.
   c) Disclose to appropriate authorities of any actual or potential danger to the User, or the environment, that they reasonably believe to be associated with software or related documents.
   d) Provide service only in their areas of competence, being honest and forthright about any limitations of their experience and education.
   e) Not knowingly use software that is obtained or retained either illegally or unethically.
   f) Use the property of the University only in ways properly authorized and with its knowledge and consent.
   g) Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.
   h) Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the organisational interest and consistent with applicable Statutes.
   i) Identify, document, collect evidence and promptly report to the Authority concerned if, in their opinion, a project or assignment undertaken is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.
   j) Accept no outside work detrimental to the work they perform for the University
   k) Strive for high quality, acceptable cost and a reasonable schedule, ensuring proper and achievable goals and objectives for any project or assignment on which they work
   l) Ensure adequate testing, debugging, and review of software and related documents on which they work.
   m) Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.
   n) Maintain the integrity of data, being sensitive to outdated or flawed occurrences.
   o) Treat all forms of software and hardware maintenance with the same professionalism as new development.
   p) Not ask any colleague (IT Professional) to do anything inconsistent with this Code.
   q) Not promote their own interest at the expense of the University.
   r) Review the work of members of the Team in an objective, candid, and properly-documented way.
   s) Report significant violations of this Code to appropriate authorities

2. The IT Professionals holding independent responsibilities (whether or not formally designated) may have to access User's electronic information, some of which may be personal and confidential, in order to develop, test, implement and support the University's applications, systems and networks and to ensure they run properly; to protect against threats such as attacks, malware, and viruses; to protect the integrity and security of information; to help support business continuity; and to help deal with threats to campus safety and the safety of individuals. In this context the designated IT Professionals shall adhere to the additional Code of Conduct as specified hereunder:
   i. Obtain the information only to the extent required to perform the assigned job/service and use the same only for the purpose for which it was obtained, properly protect the information while in possession, and dispose of it properly once it is no longer needed.
   ii. Do not peruse or examine User's electronic information for any purpose other than to address a specific issue

The accountability for the Conduct of IT Professionals of assigned responsibilities will include the following. The listing however is only representative and not exhaustive.

A. Technicians /Service Engineers

a) Never request or ask a User for their password or PIN and must not observe a User entering their password or PIN
b) Do not open emails or files while troubleshooting an issue unless the User gives specific permission and must examine only the content of emails or files as required to troubleshoot a particular problem
c) Remote access to a desktop for support purposes can only occur with the approval of the End-User via a specific desktop prompt

B. Quality Engineers, Developers, Project Managers and Analysts

a) When developing, testing analysing, maintaining or troubleshooting issues in University applications, records should be interrogated only if they are related to the problem being investigated.
b) When showing examples of pages, files, business flow or report output in documentation, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data
c) For purpose of presentation, development, testing, analysing, maintaining, or troubleshooting, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data

C. Network Engineers

a) Data traversing the network must not be monitored except for maintenance, specific diagnostics and system protection purposes (e.g. virus protection scanning)
b) Access to log information must only be used for specific purposes and as required to support the integrity of systems

D. Helpdesk Staff

a) Never ask users for passwords or PINs
b) Only enable email forwarding to another designation as may be requested by the User

E. System and Data Base Administrators

a) Data contained in log files and databases should not be disclosed beyond the need of the IT group to develop, maintain, troubleshoot or perform diagnostics unless under direction from the appropriate Authority of the OIT
b) Information about a specific user's access to networks, systems, databases, or any other computer-based resources must not be disclosed to anyone beyond the owner unless under direction from the appropriate Authority of the OIT or for the purposes of development, testing, maintenance, protection and support of an IT system

c) The casual viewing of any data contained in logs or databases that fall outside of the IT Professional's job responsibilities is strictly prohibited

F. Production Control and Computer Operations

a) All physical access to University IT Data Centres must follow established access management protocols; all requests for access from unauthorized individuals must be referred to a supervisor or manager
b) All requests for access to systems must follow established access management protocols; all requests for systems access that fall outside of the specific ones covered by the access management protocol must be referred to a supervisor or manager
c) All requests for privileged access to production systems must follow the established procedures for granting such access, including the timely and accurate logging of the request and the timely reverting of privileges upon completion of the work that prompted the request for privileged access

G. Security Engineers

a) All IT Professionals assigned with IT Security function shall adhere to a stringent code of ethics of honesty, integrity, competence, diligence justification and legality.
b) When launching an investigation in response to an alert about possible malicious activity (from an automated tool, a user, or a third party), security engineers must act in a responsible and ethical manner, specifically:
    i. Investigate only within the scope that has been identified by the alert and for the identified reason
    ii. Track the malicious activity to an originating machine and contact the owner and their IT support, sharing the information and assisting in a resolution process
c) Should an individual decline to participate in the resolution, security engineers must:
    i. Launch an escalation process to obtain management approval prior to further action
    ii. Follow the defined escalation path in consultation with the Director OIT
d) When conducting forensics on an acquired computer, security engineers must:
    i. Limit their investigative activities narrowly, working on only relevant information
    ii. Look at individual personal information only if it is required for the investigation.
    iii. Keep physical and digital investigation materials (e.g., copy of a hard drive) securely locked
    iv. Maintain a chain of custody for evidence, requiring responsibility and signoff for each step of the process.

3. If a need arises for exception to any of the ethical and procedural conduct specified in this Code of Conduct document, under any particular exigencies, prior approval must be obtained from the Director of the OIT and on matters having any legal implication additional approval of the Law Officer and the Vice Chancellor of the University must also be taken.

4. The IT Professionals shall also be bound by the prescribed Code of Conduct for End Users with reference to and in respect of their role as User to the extent applicable.

5. Any violation of this Code of Conduct if proved shall be punishable appropriately including termination from service and other legal actions.

(Dr Anil Joseph Pinto) 6/12/2021
Registrar
Registrar
CHRIST (Deemed to be University)
Bengaluru - 560 029