

#### **From the John A. Logan College Information Security Plan – Section 4: User Responsibilities**

John A. Logan College has an obligation to preserve the confidentiality of information assets owned or entrusted by the College. Information security policies and procedures have been developed to allow the College to satisfy its legal and ethical responsibilities, regarding information resources.

All College employees are required to abide by the College's Information Security Plan, as well as any other College policies, as terms of their employment. All employees share responsibility for the security of the information resources they use.

All individuals who have access to information assets are expected to use these shared resources with consideration for others. Users are expected to be informed, and act in a responsible manner, to protect their own information resources in any environment, shared or stand alone. It is unacceptable for anyone to use information resources to violate any law or College policy, or to engage in unethical activities.

Information security is every user's responsibility. If an individual finds any evidence suggesting a data breach or any other security incident may have occurred, they must contact the Help Desk by email: [helpdesk@jalc.edu](mailto:helpdesk@jalc.edu), or phone: 8388, as soon as possible.

All College employees are required to sign and submit this Confidentiality Agreement at the time of hire, and annually thereafter.

Any College employee, student or non-college individual with access to College data who engages in unauthorized use, disclosure, alteration, or destruction of data, is in violation of the College's ISP, and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.