

Corporate Compliance

Authorization for Electronic Monitoring

Purpose:

DePaul (sometimes referred to as “Organization” or “The Organization”) recognizes that a critical aspect of its Compliance Program is the establishment of a culture that promotes prevention, detection, and resolution of instances of conduct that do not conform to Federal and State requirements, DePaul’s ethical and business policies, and fraud, waste, and abuse prevention.

To promote this culture, DePaul has established a process to ensure that electronic monitoring activities are conducted ethically, legally, and with appropriate oversight and approval.

For purposes of this Policy, the term “Affected Individuals” includes all persons who are affected by the required provider’s risk areas including the required provider’s employees, the president and other senior administrators, managers, contractors, agents, subcontractors, independent contractors, and governing body and corporate officers.

Policy:

It is the Policy of DePaul to maintain a formal electronic monitoring authorization process that applies to all involved in the initiation, access or review of electronic monitoring systems, including but not limited to:

- Computers, laptops, tablets, and mobile phones
- Email and instant messaging platforms (e.g. Outlook, Teams, Slack)
- Internet access and web browsing
- File transfers, downloads and uploads
- Telephones and voicemail systems
- Video Conferencing platforms (e.g. Teams, Zoom, Webex)
- Remote access and virtual desktop environments
- Cloud based tools and storage platforms

Procedures:

I. *Authorization Process:*

1. All monitoring activities must be authorized and approved by two Vice Presidents or one Vice President and the President.
 - The primary authorizer should be the department or program Vice President as appropriate, and the secondary authorizer must be one of the following: Vice President of Human Resources, Chief Legal Officer, or Compliance Officer.
2. All authorizers must be trained in privacy and monitoring policies and have no conflict of interest in the monitoring request.
3. If the monitoring request relates to the Compliance Officer, the President and Chief Legal Officer are to be notified and must authorize the monitoring request.
4. If the monitoring request relates to the Chief Legal Officer, The Compliance Officer and President are to be notified and must authorize the monitoring request.

5. If the monitoring request relates to the President, the Compliance Officer and Chief Legal Officer are to be notified and must authorize the monitoring request. The Compliance Officer shall report such information to the President of the Board of Directors as appropriate.
6. The initiation of a monitoring request must be submitted via a secure form or system. The request must include purpose, scope, duration and justification for the review. Both authorizers must digitally sign or approve of the request. If either denies, the monitoring should not proceed, and the request should be forwarded to the President for discussion and final determination. All monitoring requests must be logged.
7. The Chief Information Officer will ensure that all requests, approvals, and disapprovals of monitoring activities as defined by this Policy are recorded, tracked and maintained.
8. Knowledge of a violation or potential violation of this Policy must be reported directly to the Compliance Officer or the Compliance Hotline.
9. DePaul strictly prohibits its management staff, employees, and Board members from initiating electronic monitoring as an act of retribution, retaliation or intimidation.