RYLEM STAFFING

Security and Privacy Policy

All contingent workers must:

- Protect and responsibly use both the physical and intellectual assets of Rylem and the Client, including property, supplies, and equipment when authorized to use such assets.
- Use Rylem and the Client provided information technology and systems (including email) only for authorized business-related purposes. Rylem strictly prohibits contingent workers from using Client-provided technology and systems to create, access, store, print, solicit or send any material that is intimidating, harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate.
- Comply with all Rylem and the Client's requirements for maintenance of passwords, confidentiality, security and privacy procedures as a condition of receiving access to The Client's internal corporate network, systems and buildings. All data stored or transmitted on the Client's owned or leased equipment is to be considered private and is the property of the Client's. The Client may monitor all use of the Client's networks and systems (including email) and access all data stored or transmitted using the Client's network. contingent workers should not expect privacy when using the Client's information technology and systems.
- Implement Security Controls to protect Personal Data and Systems when accessing/using Systems or processing Personal Data.
- Comply with Information Audit as required by the Client.
- Personal Data shall be processed for the sole benefit of the Client and for business purpose only.
- Only install software packages or permit automatic software installation routines on the Client's computers to which they have access after obtaining permission from the Client's Technology Department. Contingent workers are permitted to use the internet on the Client's computers to which they have access. However, all such internet usage must be conducted in a professional manner. Contingent workers who are required to use Office Communicator during their placement must ensure that they use this tool solely for business-related communications.
- Any device owned by the contingent worker or the Client's-provided device that accesses, transmits, or stores the Client's information, may be monitored or accessed without further notification. Contingent workers should not expect privacy in data, information, or communications accessed by, transmitted by, or stored on any device. For example, the Client's may be able to:
- See, intercept, or access any data, information, or communications accessed by or transmitted to or from the devices contingent workers use;
- Detect the removal of software restrictions imposed by the operating system (i.e., "jailbreaking");
- Permanently delete (i.e., "wipe") or return all data on the devices contingent workers use, including personal data; and
- Monitor or block the devices contingent workers use from accessing the Client's or third-party websites or services.
- In rare cases, it may be necessary for the Client's to take possession of a device used by a contingent worker in connection with an investigation or a criminal, civil or administrative proceeding. If this becomes necessary, the contingent worker will be required to provide the Client's (or its designee) temporary possession of the contingent worker's device by an agreed upon date. The contingent worker must not delete or modify any data, information, or communication stored on the device after receiving such a request from the Client. When the device is in the Client's possession The Client may release data, information or communications gathered from the contingent worker's device to third parties related to the relevant proceeding. Agency Employee's signature below constitute acceptance of the terms specified within this Agreement.