Information Systems Security Statement

HDR is committed to maintaining information systems security practices that protect our data and support our clients' security needs.

We recognize that protecting client and HDR data is critical to our mutual success. HDR's information security systems controls and processes govern both employee and contractor use of information systems and establish requirements for protecting technology assets, access to information systems, and the proper use of company business information.

HDR expects all employees to act with integrity and requires all employees to follow the HDR Code of Business Ethics and Conduct. Cybersecurity awareness, email and other security essentials training is assigned to all new hires and all HDR employees are required to acknowledge their information systems security responsibilities.

HDR has implemented security controls and processes that comply with key government and industry data protection regulations and standards. Cybersecurity controls and processes implemented at HDR include, but are not limited to, the following:

- Security software that monitors, detects, and prevents potential malicious intrusion
- Penetration and vulnerability testing, including simulated phishing
- Mobile device management (MDM) on HDR phones and tablets
- Identity and access management, including strong passwords and multi-factor authentication
- Computer screen locks and laptop encryption
- Anti-virus software, web and spam filtering, and firewalls
- Cybersecurity employee training and threat awareness
- Timely software patching
- Regularly scheduled backups for recovery of data

Regular audits are conducted to align our controls with relevant industry and government regulations and to improve our information systems security controls and processes.

John W. Henderson
Chief Executive Officer

January 01, 2025