Updated: April 2026

Cybersecurity Policy

Purpose and Commitment

Universal Display Corporation and its worldwide subsidiaries (collectively, UDC) are committed to protecting the confidentiality, integrity, and availability of UDC information and information entrusted to UDC by employees, partners, and other stakeholders. UDC views cybersecurity as a business risk and a business enabler, using a defense-in-depth approach. UDC invests in people, processes, and technology to reduce the likelihood and impact of cyber incidents.

Governance and Oversight

Cybersecurity is governed through an enterprise risk lens with executive management accountability and board-level oversight. The Audit Committee of the Board of Directors provides oversight of the cybersecurity program at UDC and receives periodic updates on cybersecurity risk, material initiatives, and key program metrics. Management is responsible for executing the cybersecurity program and reporting significant developments.

Risk Management Approach and Frameworks

UDC manages cybersecurity through a continuous risk management program that includes identifying relevant threats, assessing risk, prioritizing controls and investments, and measuring progress over time. UDC's program is informed by widely recognized security frameworks and standards and UDC maintains written policies and standards to operationalize requirements across the organization.

Core Program Pillars (How Data Is Protected)

UDC's cybersecurity program is built on layered safeguards designed to prevent unauthorized access, reduce attack surface, and limit the impact of disruptions:

- **Identity & Access Security.** UDC implements access controls and authentication practices intended to ensure only authorized employees

can access UDC systems and data, and that access is appropriate to job responsibilities (least privilege).

- **Endpoint, Network, and Monitoring Controls.** UDC employs a combination of preventive and detective controls to help protect endpoints and networks, including configuration standards, monitoring, and alerting to identify suspicious activity.
- **Data Protection.** UDC uses administrative, technical, and physical safeguards to help protect sensitive UDC information and to reduce the risk of unauthorized disclosure. This includes controls for acceptable use in regard to computing and the use of generative artificial intelligence, secure collaboration, and appropriate retention/disposal practices.
- **Vulnerability and Change Management.** UDC maintains processes for assessing vulnerabilities and managing changes to production systems in a controlled manner, helping reduce risk introduced by misconfiguration or unpatched weaknesses.
- **Security awareness and culture.** UDC requires periodic security awareness education for personnel and reinforces user responsibilities such as reporting suspicious activity promptly.
- **Third-Party Risk Management.** UDC assesses cybersecurity risk when engaging third-party service providers and incorporates vendor security considerations into its technology and business decision-making processes. Appropriate safeguards are expected to help protect UDC systems and information when third parties are involved.

Incident Response

Despite strong controls, cybersecurity incidents can occur. UDC maintains an incident response program designed to identify, contain, eradicate, recover from, and learn from cybersecurity incidents. UDC's cybersecurity incident response policy defines governance, roles and responsibilities, communication & escalation pathways, and post incident review expectations.

Training

All personnel with access to UDC data are required to complete periodic cybersecurity training. This training is provided through regular computer-based training and targeted simulation exercises.

Continuous Improvement and Investment

Cybersecurity is an ongoing program. UDC periodically assesses maturity and risk, tracks remediation and improvement initiatives, and maintains a roadmap of prioritized investments (people, process, and technology) to strengthen our security posture over time.

UDC reviews this policy periodically and we reserve the right to update, change or replace any part of it any time, at our discretion, with or without prior notice.