# InterDigital, Inc.
# Cybersecurity Policy

At InterDigital, we take a defense-in-depth approach to protect our data, our customer's data, our infrastructure, and our employees. We embed data protection throughout our operations and information technology programs, relying on multiple and various controls to prevent and detect threats, with the goal of safeguarding our assets, data and personnel. This Cybersecurity Policy, and the other policies and standards it references, are applicable to InterDigital and all of its business lines, subsidiaries, and affiliates.

## Policy & Governance

We embed data protection throughout our business operations and information technology program. Our goal is to provide a disciplined approach to safeguarding our information assets, customer data and employees. This includes a commitment to the privacy of any data as outlined in our Privacy Policy. InterDigital does not rent, sell, or provide personal data to third parties for purposes other than as required for completing transactions or providing services. We minimize the collection and retention of this data as outlined in our Privacy Policy. Our Cybersecurity Program is governed by the Audit Committee of our Board. The Audit Committee of the Board and the full Board each receive quarterly updates on cybersecurity and privacy risks.

As a foundation to this approach, InterDigital maintains a comprehensive set of cybersecurity policies and standards. These policies and standards were developed in collaboration with a wide range of disciplines, such as information technology, cybersecurity, legal, compliance and business. Our Board's Audit Committee is responsible for overseeing all aspects of our privacy and data security.

Our Cybersecurity strategy and policies are continually reassessed to ensure they identify and proactively address the constant changes in the global threatscape. This includes audits conducted no less frequently than biannually by external, independent auditors. Decision makers are regularly kept up to date on cybersecurity trends, and ongoing collaboration with stakeholders throughout the business help ensure continued awareness and visibility of future needs.

## Technology

InterDigital utilizes sophisticated technologies and tools to protect its environment, including multifactor authentication, firewalls, intrusion detection and prevention systems, vulnerability and penetration testing, privilege and password management, and digital risk protection. We generally deploy strong encryption policies on our data, utilizing both encryption in transit and at rest.

Our Security Operations Center is continuously improving their detection capabilities alongside proactive threat hunting teams.

InterDigital has a robust and aggressive patch management process designed to reduce software-based vulnerabilities quickly and effectively.

## Training & Awareness

All InterDigital employees, contractors, consultants and temporary employees receive data privacy and a baseline cybersecurity training before being permitted to access InterDigital systems, typically at hire. Additionally, all employees, contractors, consultants, temporary employees and others with access to Company systems are required to take quarterly cybersecurity training refresher courses covering a broad range of security topics such as phishing, social engineering, mobile security hygiene, password protection and more.

We provide cybersecurity education through computer-based training, regular email publications, and targeted simulation exercises. All InterDigital contractors and consultants are also required to receive this periodic training, or to receive similar relevant training from their employers.

## Incident Response

InterDigital has implemented a Security Incident Response Framework. The framework is a set of coordinated procedures and tasks, including both proactive and reactive measures, that the InterDigital incident response team executes to ensure timely and accurate resolution of computer security incidents.

To maintain the robustness of the framework, we annually conduct tabletop testing exercises, using risk analysis to select which components of the framework to test.

**DATED: March 25, 2024**