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.

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.

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 Cybersecurity strategy and policies are continually re-assessed to ensure they identify and proactively address the constant changes in the global threatscape. 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.

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 are required to take data privacy and a baseline cybersecurity training at hire. Additionally, all employees 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 educate employees through computer-based training, regular email publications, and targeted simulation exercises. Certain InterDigital contractors and consultants receive this training as well.

Incident Response

InterDigital has implemented a Security Incident Response Framework. The framework is a set of coordinated procedures and tasks 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: February 23, 2021