WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.

- We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.

- We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

WE WILL OPPOSE CRIMINAL AND GOVERNMENT EFFORTS TO ATTACK USERS AND CUSTOMERS ANYWHERE.

- We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.

- We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.

- We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.

- We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

- We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.

- We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

To ensure a meaningful partnership is established through the implementation of the Tech Accord, we, the undersigned companies, will continue to define collaborative activities we will undertake to further this Accord.

We will also report publicly on our progress in achieving these goals.
PARTICIPATING ORGANIZATIONS
PARTICIPATING ORGANIZATIONS

facebook
fastly
FireEye
Flowmon
Framework
F-Secure
Gigamon
GitHub
GitLab
Globant
GreyCortex
Deltron
guardtime
HCS
Hitachi
(H)matic
HP
Hewlett Packard Enterprise
Imperva
Indra
Minos IT
Infinit
Integrity
International Software Systems
Intuit
Juniper
Koolspan
KPN
L&L Safe Consulting Partners
LawToolBox
LinkedIn
Lexus
Lexmark
Lexmark
Mediacom Computer Works
MarkMonitor
MediaPro
Mercado Libre
Microsoft
napSolutions
NetApp
Nielsen
Nokia
Northwave
NTT
Onshore Security
Oracle
Orange
Paladion
PARTICIPATING ORGANIZATIONS

Panasonic  panda  pax8  percipient.ai  predica.
QOMPLX:  QAssociates  Resecurity  reveal.  Rockwell Automation  RSA
SAFEPC:  safetica  salesforce  SAP  Schneider Electric  Scitum
secucloud.  SecurityScorecard  SHARP  SILENT BREACH  SOND
STACKPATH  STRATA  stripe  StrongConnect  Swisscom  SWITCHFAST
Synack  TADGROUP  TANium  TIM  Telefonica  telalink
Tenable  ThreatModeler  Trend Micro  UNiSYS  US Licensing Group  US Medical IT
VAiDY  VMware  VU  VTC  WIPFLi  WIS@key