Ziff Davis Vendor Policy and Code of Conduct

(Last revised February 2022)

1. **Purpose and Overview**

This Vendor Policy and Code of Conduct ("Policy") sets forth the expectations applicable to the Vendors ("Vendors") of Ziff Davis, Inc. and any of its subsidiaries ("Ziff Davis").

2. **Definition**

a. "Agreement" means any written document, verbal agreement, or contract between Vendor and Ziff Davis under which Vendor performs services for Ziff Davis.

b. "Applicable Laws" refers to any and all statutes, laws, treaties, rules, codes, ordinances, regulations, permits, interpretations, certificates, judgements, decrees, injunctions, writs, orders, subpoenas, or like action of a government authority applicable to: (i) the Agreement and/or this Policy; (ii) the performance of obligations or other activities by Vendor related to the Agreement; and (iii) a party, a party's affiliates (if any), a party's subcontractors (if any), or to any of their representatives, including but not limited to the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CPPA), United States state data breach notification laws, Canada's law on Personal Information Protection and Electronics Document Act (PIPEDA), the EU Directive 96/46/EC and the EU General Data Protection Regulation. To the extent that Protected Health Information is being disclosed by Ziff Davis pursuant to the Agreement, applicable laws also include: the Health Insurance Portability and Accountability Act of 1996, The Health Information Technology for Economic and Clinical Health ("HITECH") Act, and the Privacy and Security Rule regulations of HIPAA and the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and all amendments to and further regulations of the HIPAA and HITECH Acts (collectively, "HIPAA")

c. "Attestation of Compliance" refers to the Payment Card Industry Data Security Standards (PCI DSS) Attestation of Compliance. If the Vendor will be receiving, storing and/or processing credit card information on behalf of Ziff Davis, Vendors must complete this declaration annually to confirm that they are in agreement with the Data Security Standards for handling credit card data electronically.

d. "Business Associate" refers to a person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides services to, a covered entity as defined under HIPAA.

e. "HIPAA Business Associate Agreement" refers to the contract between a HIPAA- covered entity and a HIPAA Business Associate required under HIPAA.

f. "Business Continuity and Disaster Recovery" refers to the practices in which Vendor prepares for unforeseen risks to continue operations including: (i) specific steps taken to resume operations in the event of a natural disaster, national emergency, or threats to a company's normal operations; and (ii) the processes and procedures an organization must put

in place to ensure that critical functions can continue during and after one of these events.

g. "Personal Information" means any information or data provided by Ziff Davis and its affiliates or collected or received by Vendor on behalf of Ziff Davis that identifies, or when used alone or in combination with other information, reasonably identifies an individual person, or any other data considered to be personal data as defined under Applicable Laws. Personal Information may include, but is not limited to: (i) a first or last name or initials; (ii) a home or other physical address, including street name and name of city or town; (iii) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (iv) a telephone number; (v) a social security number, tax ID number or other government-issued identifier; (vi) an Internet Protocol ("IP") address or host name that identifies an individual; (vii) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (viii) birth dates or treatment dates; or(ix) coded data that is derived from Personal Information. Additionally, to the extent any other information (such as, but not necessarily limited to, case report form information, clinical trial identification codes, personal profile information, IP addresses, other unique identifiers, or biometric information) is associated, combined with or otherwise reasonably linkable to Personal Information, then such information also will be considered Personal Information.

h. "Protected Health Information" means any information, whether oral or recorded in any form or medium, that: (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (ii) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. This information becomes protected when it is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. The foregoing definition aligns with the HIPAA standard of Protected Health Information, and is subject to change in the event applicable laws are put into place to modify the foregoing definition.

i. "Processing of Personal Information (Processing)" refers to any operations which are performed upon Ziff Davis Information, including, but not limited to, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking or dispersed erasure, or destruction.

j. "Sensitive Personal Information" means any Personal Information that requires additional privacy and security protections, which includes:

   i. All government issued identification numbers;
   ii. All financial account numbers;
   iii. Individual medical records and biometric information;
   iv. Reports of individual background checks and all other data obtained from a U.S. consumer reporting agency and subject to the Fair Credit Reporting Act;
   v. Data elements revealing race, ethnicity, national origin, religion, philosophical beliefs, trade union membership, political orientation, sex life or sexual orientation, criminal records, histories of prosecutions or convictions, or allegations of crimes;
   vi. Any information deemed to be sensitive data under Applicable Laws; and
   vii. Any other information designated by Ziff Davis as Sensitive Personal Information.

k. "Ziff Davis Information" refers to any Personal Information, Protected Health Information, Sensitive Personal Information or other confidential information provided by Ziff Davis and/or its affiliates and subsidiaries, either directly or indirectly in any form, and any data, materials, processes, or information a Vendor develops for us or receives as a result of this relationship that does not fall under Personal Information, Protected Health Information or Sensitive Personal Information.

3. **Minimum Information Security Controls.**

Vendor must implement and maintain the minimum information security controls as set forth below.

a. Audit of Security Controls

i. Vendor shall maintain all necessary documentation to show compliance with the Policy and Code of Conduct.
ii. Additionally, upon request, Vendors shall allow Ziff Davis or an independent third party to audit Vendor's compliance with this Policy and Code of Conduct. Ziff Davis reserves the right to audit (or to engage a third party to audit) all network device configurations and administration processes at any time, including, but not limited to, inbound and outbound packets, firewalls, network peripherals and attached computer systems.
iii. If set forth in the Agreement, Vendor may be required to obtain a formal audit of the security controls conducted by an unaffiliated third party. If this is necessary, Vendor must provide Ziff Davis with written audit results. Results must be an ISO/ICE 27000/2 or other appropriate ISO/IEC certification. Vendor's information security management program must comply with internationally recognized, generally applicable ISO/IEC standards.
iv. If any such audit reveals material gaps or weaknesses in Vendor's security program, Ziff Davis shall be entitled to suspend transmission of Ziff Davis Information to Vendor and Ziff Davis may, at its election, terminate the Agreement without penalty. Vendor's Processing of any of this information is to cease until such issues are resolved to the satisfaction of Ziff Davis.

b. Security Management

Vendors must have a comprehensive written information security program, based on best practice standards for their industry. The program must contain:

i. Written information privacy and security policies that are revised on a regular basis and regularly communicated to appropriate personnel and third party providers and;
ii. Security training and awareness activities performed regularly and designed to enable employees and contractors to identify information privacy risks.

c. Risk Management

Vendors must perform periodic risk assessments to evaluate the risk profile regarding the collection, storage, and use of Ziff Davis Information.

i. Risk Mitigation. Vendors must continually identify and mitigate internal and external risks that could result in the compromise of confidential information, including Ziff

Davis Information.

ii. Risk Assessment. Vendors must conduct regular information privacy and security risk assessments in each area of proper operation.

iii. Media Sanitization. Vendors must ensure that media sanitization conforms to NIST SP 800-88, Media Sanitization, or any successor standard.

d. Personnel Security/ Human Resources Security

Vendor shall implement controls to enable employees, contractors, and service providers to adhere to policies and standards according to roles and access and to reduce the risk of theft, fraud, loss, and misuse of facilities or information.

i. Vendor must ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles for which they are considered, including through any appropriate personnel screening.

ii. Vendor shall appoint, properly train and identify to Ziff Davis in writing an individual within Vendor's organization who is authorized to respond to inquiries from any data protection authority, Vendor, or a data subject concerning Vendor's collection, access, use, storage, and/or transfer of Personal Information. Vendor will deal promptly with all inquiries relating to Personal Information and provide all required information to Ziff Davis.

iii. Security roles and responsibilities of employees, contractors and third party users must be defined and documented to incorporate Ziff Davis data protection control requirements including background checks to the extent permitted by applicable law.

iv. All employees, contractors, and third-party users must be notified of the consequences for not following this Policy and Code of Conduct in connection with the handling of Ziff Davis Information.

v. All assets used to manage or store Ziff Davis Information must be protected against unauthorized access, disclosure, modification, destruction or interference.

vi. All employees, contractors and third-party users must be provided with education and training in privacy and security procedures and the correct information Processing requirements.

vii. If Vendor has knowledge that an agent is using or disclosing Ziff Davis Information in a manner contrary to this Policy and Code of Conduct, Vendor will take reasonable steps to prevent or stop the use or disclosure.

e. Operations Management

i. Vendor must provide appropriate security and protection from unauthorized access, damages and interference of assets based on classification, information sensitivity, and other factors.

ii. All software used by Vendor in providing services to Ziff Davis must be properly licensed before entering into an Agreement with Ziff Davis.

iii. Vendor is responsible for data protection, privacy compliance, and security control validation/certification of its sub-contractors.

iv. Vendor will protect against the risk of malicious code by using anti-virus products on clients and servers; use an appropriate blocking strategy on the network perimeter; filtering input to applications; and creating, implementing and training staff in appropriate computing policies and practices.

f. Security Breach

i. Security Breach. Vendor must comply with specified incident response processes for Ziff Davis Information and Ziff Davis systems. Vendor shall follow documented responsibilities and procedures to respond to information security incidents quickly, effectively, and in an orderly way. "Security Breach" means any act or omission that compromises either the security, confidentiality or integrity of the Ziff Davis Information or the physical, technical, administrative or organizational safeguards put in place that relate to the security, confidentiality, or integrity of the Ziff Davis Information.

ii. Cost Allocation. Vendor shall bear all costs associated with resolving a Security Breach, including those costs associated with conducting an investigation, notifying consumers and others as required by law or the Payment Card Industry Data Security Standard, providing consumers with one year of credit monitoring, and responding to consumer, regulator and media inquiries.

iii. Reporting. Vendor shall report any Security Breach through appropriate management channels as quickly as possible. Any Security Breach involving or impacting Ziff Davis or a Ziff Davis affiliate or subsidiary must be reported to Ziff Davis. Notification must be within twenty-four (24) hours from detection if Ziff Davis Information, the Ziff Davis brand, logo or trademarks are involved or compromised.

iv. Cooperation with Ziff Davis. Vendor shall cooperate with Ziff Davis in investigations of any incidents involving Ziff Davis Information or Ziff Davis systems. Vendor shall cooperate with Ziff Davis and Ziff Davis employees, affiliates and representatives in responding to inquiries, claims, and complaints regarding the Processing of Ziff Davis Information, including, but not limited to: (a) assisting with any investigation as requested by Ziff Davis; (b) providing Ziff Davis with physical access to facilities and operations affected; (c) facilitating interviews with Vendor's representatives and others involved in the matter; and (d) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably requested by Ziff Davis.

v. Providing Notice to Third Parties. Vendor shall not inform any third party of any Security Breach which affects Ziff Davis, without first obtaining the prior written consent of Ziff Davis, other than to inform a complainant that the matter has been forwarded to Ziff Davis' legal counsel. Ziff Davis shall have the sole right and authority to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Ziff Davis' discretion; (ii) the contents of such notice; (iii) whether any remediation may be offered to affected persons; and (iv) the nature and extent of any such remediation.

g. Encryption and Data Management Controls

i. Cryptographic controls must be used to protect the confidentiality, integrity, and availability of Ziff Davis Information in transit and while in Vendor's possession. Controls for the management and use of cryptographic keys must be developed, implemented, and reviewed by Vendor on a periodic basis.

ii. Vendor must encrypt: (i) laptops and all other portable devices storing Ziff Davis Information which is Personal Information; as well as (ii) files containing Ziff Davis Information on all laptops or other portable devices; (iii) all messages containing

Ziff Davis Information (or files containing Personal Information) during transit over public networks; and (iv) all files containing Personal Information included in a message sent over public networks.

iii. If the Processing involves the transmission of Ziff Davis Information over a network, Vendor shall have implemented appropriate supplementary measures to protect the Ziff Davis Information against the specific risks presented by the Processing. Ziff Davis Information may only be transmitted in an encrypted format.

iv. Ziff Davis Information may not be stored on any portable computer devices or media (including laptop computers, removable hard disks or flash drives, personal digital assistants (PDAs) or computer tapes) unless the Ziff Davis Information is encrypted, or the hard drive that contains the Ziff Davis Information on the portable computer device or media is fully encrypted.

v. Vendor should also be aware of any regulations, standards, or industry or sector specific guidelines that set forth minimum guidelines for encrypting personal data.

h. Access Controls

Access to resources including Ziff Davis Information must be regulated through the use of information security access controls and authorization mechanisms commensurate with risk.

i. General. Vendor will secure its computer networks using multiple layers of access controls to protect against unauthorized access. In particular, Vendor will: (i) group network servers, applications, data and users into security domains; (ii) establish appropriate access requirements within and between each security domain; and (iii) implement appropriate technological controls to meet those access requirements consistently; including (for example) firewalls.

ii. Remote Access. Vendor will secure remote access, with multi-factor authentication, to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging and monitoring access events and subsequent audits.

iii. Password Policy. Vendor must limit access to the minimum necessary to perform the required function. Vendor must maintain and enforce a password policy which addresses password length, composition, complexity, lockout, history and expiration.

iv. Termination of Access. Vendor must revoke access for any Vendor employee, contractor, or third-party user to Ziff Davis Information, and facilities which process Ziff Davis Information, or provide access to Ziff Davis systems upon termination of their employment, contract or agreement, or adjust access upon a change of responsibility.

v. Security Zones. Vendor will define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.

vi. Firewalls. Vendor must appropriately leverage firewall infrastructure to segregate sensitive environments and restrict the use of insecure protocols. Network segments connected to the internet must be protected by a firewall which is configured to secure all devices behind it.

vii. Business Continuity and Disaster Recovery. Vendor must have appropriate Business Continuity and Disaster Recovery capabilities to prevent or mitigate business interruption and associated impact. Vendor must test the Business Continuity and

Disaster Recovery capability regularly.

viii. Vendor must counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters and ensure their timely resumption.

ix. Vendor shall have an established disaster recovery/business continuity plan that addresses ongoing access to the Ziff Davis Information as well as security needs for backup sites and alternative communication networks.

i. Compliance

i. Information security and data protection controls and processes must comply with Applicable Law and contractual obligations, to avoid a breach and compromise of Ziff Davis Information. Vendor must comply with all changes in applicable laws of which Vendor is notified. If Vendor is unable to do so, it must notify Ziff Davis immediately and Ziff Davis may terminate the Agreement, unless the parties mutually agree in writing upon steps to be taken to enable Vendor to so comply.

ii. Ziff Davis Privacy Policy. Vendor shall only use Ziff Davis Information in accordance with the Ziff Davis Privacy Policy, as amended and updated from time to time.

iii. PCI Data Security Standards. If Vendor has access to or will create, receive, store, process, or transmit Ziff Davis cardholder information (e.g. credit, debit, stored value, or prepaid card information), Vendor, at its own expense, warrants:

(a) Vendor is, and will remain, responsible for securing cardholder information in its care, custody, possession, or control;

(b) Vendor will comply with the applicable current Payment Card Industry Data Security Standards ("PCI Standards"); and

(c) Vendor will provide Ziff Davis with an annual third-party Attestation of Compliance. If a third-party provider will have access to or will create, receive, store, process, or transmit Ziff Davis cardholder information to perform under the Agreement, Vendor warrants that it will require this of the third party provider and will provide Ziff Davis with the third party provider's annual Attestation of Compliance issued by another party unaffiliated with the third party provider.

iv. HIPAA Protected Health Information. If Vendor has access to or will create, receive, store, process, or transmit Protected Health Information, Vendor, at its expense, warrants:

(a) Vendor is, and will remain, responsible for securing Personal Health Information in its care, custody, possession or control;

(b) Vendor will comply with HIPAA, including all applicable privacy and security standards; and

(c) Vendor will sign the Ziff Davis HIPAA Business Associate Agreement.

j. International Law. To the extent that the scope of the Agreement between Ziff Davis and

Vendor extends beyond the United States, the following applies:

i. Vendor shall not transfer Ziff Davis Information across any national borders or permit remote access to the Ziff Davis Information by any employee, contractor, or another third party unless Vendor has the prior written consent of Ziff Davis for such transfer or access.

ii. If Vendor has access to or will create, receive, store, process, or transmit Ziff Davis Information of customers in non-US countries, Vendor represents and warrants that all Processing, storage, retention, and destruction of personal data by Vendor and third-party providers will be in compliance with all then-current applicable international, federal, provincial, state, and local laws, rules, regulations, and ordinances, including without limitation, data breach notification laws. For the purpose of clarification and without limiting the preceding, if Vendor collects, receives, processes, stores, retains, or destroys Ziff Davis Information of any citizen of Canada, Mexico or the European Union in connection with performing services for Ziff Davis, then the following provisions apply:

(a) All Processing, storage, retention and disposal of Ziff Davis Information of citizens of Canada will comply with Canada's law on Personal Information Protection and Electronics Document Act ("PIPEDA") and any provincial laws which may apply based on location;

(b) All Processing, storage, retention and disposal of Ziff Davis Information of citizens of European Union comply with the EU Directive 95/46/EC and the General Data Protection Regulation, including all implementing legislation and successor statutes, laws, rules, regulations, and directives.

4. **Insurance**

a. Vendor shall, at its own cost, take out and maintain cybersecurity insurance on terms reasonably satisfactory to Ziff Davis, with a reputable insurer. Such insurance shall cover any and all losses, claims, demands, proceedings, damages or costs arising from or in connection with breach of this Policy and Code of Conduct.

b. Vendor shall ensure that the beneficial interest of Ziff Davis is noted on the face of the insurance policy and shall make full details of the insurance and proof of payment of the insurance premium available to Ziff Davis on request.

5. **Code of Conduct**

a. Vendors are expected to act in accordance with Ziff Davis' Code of Business Conduct and Ethics (available at www.ziffdavis.com).

b. Vendors are expected to act in accordance with Ziff Davis' Labor Rights Policy (available at www.ziffdavis.com), including but not limited to provisions on freedom of association and collective bargaining, and provisions prohibiting the use of forced labor, child labor exploitative practices, human trafficking or modern slavery. Ziff Davis also expects its Vendors to comply with applicable laws on working hours, minimum wages, acceptable living conditions and disciplinary practices (including where applicable

corporal punishment), and further expects Vendors to comply with ILO standards.

c. Vendors are expected to act in accordance with Ziff Davis' Human Rights Policy (available at www.ziffdavis.com).

d. Vendors are expected to act in accordance with Ziff Davis' Environmental Policy and Ziff Davis' Climate Change Policy Statement (available at www.ziffdavis.com).

e. Vendors are expected to act in accordance with Ziff Davis' corporate policies prohibiting discrimination or harassment (available at www.ziffdavis.com).

f. Vendors are expected to act in accordance with Ziff Davis' Whistleblower Policy (available at www.ziffdavis.com). More information on Ziff Davis' whistleblower program can be found at https://secure.ethicspoint.com/domain/media/en/gui/46008/index.html.

g. Vendors are expected to act in accordance with Ziff Davis's Export Compliance Manual (available at www.ziffdavis.com) and must comply with all U.S. export controls. Vendors are also expected to provide Ziff Davis with ECCNs applicable to their products and services. Ziff Davis does not do business with entities and individuals located in Cuba, the Democratic People's Republic of North Korea, Iran, Syria or the Crimea Region of Ukraine, or who are on the U.S. Treasury Department's Specially Designated Nationals list, and Ziff Davis expects its vendors not to do so either.

6. **Amendments**

These provisions are subject to change by amendment. Vendor is responsible for complying with the most up to date version of this Policy and Code of Conduct.

7. **Waivers**

From time to time, Ziff Davis may waive certain provisions and expectations of this Policy and Code of Conduct. Any Vendor, employee or director who believes that an explicit waiver is required should discuss the matter with an Appropriate Ethics Contact, pursuant to the Company's Business Code of Conduct and Ethics.