Norton Executive Master Policy Summary of Benefits (2026)

This Summary of Benefits is provided to inform you, as a customer in good standing with Gen Digital, are enrolled for coverage under the Norton Executive Master Policy issued to Gen Digital and described herein. Various provisions in the Norton Executive Master Policy restrict coverage. Read the entire Norton Executive Master Policy carefully to determine rights, duties and what is and is not covered. This Summary of Benefits does not state all the terms, conditions, exclusions and definitions within the Norton Executive Master Policy. Your benefits will be subject to all the terms, conditions, exclusions and definitions of the Norton Executive Master Policy. A complete copy of the Norton Executive Master Policy will be available upon request. If the Norton Executive Master Policy is terminated, your benefits under the Norton Executive Master Policy will cease to be effective on that date. It is the obligation of Gen Digital to inform you of any termination of the Norton Executive Master Policy. To obtain a complete copy of the Norton Executive Master Policy as issued to Gen Digital, please contact Gen Digital.

Limits of Liability:

Security and Privacy Liability Coverage	$250,000
Breach Event Costs Coverage	$250,000
Data Recovery Coverage	$250,000
Cyber Extortion Coverage	$250,000
Cyber Crime Coverage	$250,000
Identity Theft Expenses Coverage	$250,000
Cyber Bullying Coverage	$250,000
Annual Aggregate Limit per Named Insured:	$250,000
Deductible:	$0 each **Claim**

INSURING AGREEMENTS

(A) Security and Privacy Liability Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Damages**, including liability **Assumed Under Contract**, and related **Defense Costs**, that an **Insured** becomes legally obligated to pay as a result of a **Claim** for an actual or alleged **Security and Privacy Wrongful Act**, provided always that: (a) the **Claim** is first made against the **Insured** during the **Coverage Period**; (b) the **Claim** is reported to the Company in writing pursuant to this Policy; (c) the **Insured** had no knowledge of any circumstance, dispute, situation or incident giving rise to the **Claim** prior to the Knowledge Date set forth in the Declarations; and (d) the **Security and Privacy Wrongful Act** is committed on or after the Retroactive Date set forth in the Declarations.

(B) Breach Event Costs Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Notification Expenses** and **Breach Support and Credit Monitoring Expenses** that an **Insured** incurs because of a **Security Breach** or **Privacy Breach**, provided always that: (a) the **Insured** first discovers the **Security Breach** or **Privacy Breach** during the **Coverage Period**; and (b) the **Security Breach** or **Privacy Breach** is reported to the Company in writing pursuant to this Policy.

(C) Data Recovery Coverage

(1) Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Digital Assets Loss** and **Special Expenses** that an **Insured** incurs because of damage, alteration, corruption, distortion, theft, misuse or destruction of **Digital Assets** resulting from a **System Failure**, provided always that: (a) the **Insured** first discovers the **System Failure** during the **Coverage Period**; (b) the **System Failure** is reported to the Company in writing pursuant to this Policy; and (c) the **Insured** provides clear evidence that the **Digital Assets Loss** and **Special Expenses** directly result from a **System Failure**.

(2) The Company shall pay **Digital Assets Loss** and **Special Expenses** for up to twelve (12) months following the **Insured's** discovery of the **System Failure**, unless specified otherwise by endorsement to this Policy.

(D) Cyber Extortion Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay Cyber Extortion Expenses and Cyber Extortion Monies that an Insured incurs as a direct result of a Cyber Extortion Threat, provided always that: (a) the Insured first discovers the Cyber Extortion Threat during the Coverage Period; (b) the Cyber Extortion Threat is reported to the Company in writing pursuant to this Policy; and (c) the Insured makes every reasonable effort to notify local law

enforcement authorities and the Federal Bureau of Investigation before surrendering any Cyber Extortion Monies in response to a Cyber Extortion Threat.

(E) Cyber Crime Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Financial Fraud Loss** that an **Insured** sustains because of **Financial Fraud**, provided always that: (a) the **Insured** first discovers the **Financial Fraud** during the **Coverage Period**; (b) the **Financial Fraud** is reported to the Company in writing pursuant to this Policy; and (c) the **Insured** provides written confirmation to the Company that the **Insured's** bank or credit card company has refused to reverse or prevent a payment transaction or to indemnify or reimburse the **Insured** for the **Financial Fraud Loss**.

(F) Identity Theft Expenses Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Identity Theft Expenses** that an **Insured** incurs because of **Identity Theft**, provided always that: (a) the **Insured** first discovers the **Identity Theft** during the **Coverage Period**; and (b) the **Identity Theft** is reported to the Company in writing pursuant to this Policy.

(G) Cyber Bullying Coverage

Subject to the applicable Deductible and Limit of Liability, the Company shall pay **Cyber Bullying Expenses** that an **Insured** incurs because of a **Cyber Bullying Incident**, provided always that: (a) the **Insured** first discovers the **Cyber Bullying Incident** during the **Coverage Period**; and (b) the **Cyber Bullying Incident** is reported to the Company in writing pursuant to this Policy.

DEFINITIONS

As used in this Policy:

(1) **"Account Manager"** means any person or organization authorized by an **Insured** to request (a) the transfer, payment or delivery of **Money** or **Securities** from a **Covered Bank Account** or (b) the transfer, payment or delivery of cryptocurrency from an **Insured's** cryptocurrency wallet.

(2) **"Act of Cyber Terrorism"** means the premeditated use of disruptive activities, or the threat to use disruptive activities, against a **Computer System**, including any associated network and **Data** stored thereon, with the intention to cause harm, to further social, ideological, religious, political, or similar objectives, or to intimidate any person in furtherance of such objectives; provided that such activities are not committed by, or at the express direction of, a sovereign state or a government simultaneously engaged in **War** or a **Cyber Operation** carried out as part of any **War**.

(3) **"Application Program"** means any computer software program that performs a particular function or task within the **Computer Operating System** for the end-user, including, but not limited to, database programs, web browsers, enterprise software, word processors, graphics software and media players.

(4) **"Approval"** means the advance written agreement or consent by the Company, which will not be unreasonably withheld.

(5) **"Assumed Under Contract"** means liability for **Damages** resulting from a **Security Breach** or **Privacy Breach**, where such liability has been assumed by an **Insured** in the form of a written hold harmless or indemnity agreement, but only if such agreement was executed before the **Security Breach** or **Privacy Breach** occurred.

(6) **"Attack Vector"** means the method or combination of methods that are used in a **Hacking Attack**.

(7) **"Bodily Injury"** means physical injury, sickness, disease or death sustained by any person and, where resulting from such physical injury only, mental anguish, mental injury, shock, humiliation or emotional distress.

(8) **"Breach Support and Credit Monitoring Expenses"** means reasonable and necessary expenses that an **Insured** incurs to provide support activity to parties affected by a **Privacy Breach**, including the cost to provide a maximum of twenty-four (24) months of credit, identity or healthcare record monitoring services, fraud alert services, identity theft assistance services and credit or identity repair and restoration services. **Breach Support and Credit Monitoring Expenses** must be incurred with **Approval**.

(9) **"Business"** means any employment, trade, occupation, profession or enterprise intended to realize a benefit or financial gain, whether engaged in on a full-time, part-time, occasional or temporary basis.

(10) **"Business Identity Theft"** means the theft or unauthorized, unlawful or fraudulent use, access or transfer of a means of identifying a **Business** owned or operated by an **Insured**, with the intent to commit or aid or abet another to commit a crime, including the theft or fraudulent use of a business name, federal or state tax identification number, or other business records or information to establish corporate credit accounts, secure loans or enter contracts.

(11) **"Claim"** means:

(a) with respect to Security and Privacy Liability Coverage only:

i. a written demand made against an **Insured** for **Damages** or non-monetary relief;

ii. a written request received by an **Insured** to toll or waive a statute of limitations relating to legal proceedings against the **Insured**; or

iii. the service of a civil lawsuit or the institution of arbitration or other alternative dispute resolution proceedings against an **Insured** seeking **Damages**, a temporary restraining order or a preliminary or permanent injunction.

(b) with respect to Breach Event Costs Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of a **Security Breach** or **Privacy Breach**.

(c) with respect to Data Recovery Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of a **System Failure**.

(d) with respect to Cyber Extortion Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of a **Cyber Extortion Threat**.

(e) with respect to Cyber Crime Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of **Financial Fraud**.

(f) with respect to Identity Theft Expenses Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of **Identity Theft**.

(g) with respect to Cyber Bullying Coverage only, written notice from an **Insured** or an **Insured's** representatives to the Company of a **Cyber Bullying Incident**.

A **Claim** under the Security and Privacy Liability Insuring Agreement of this Policy will be deemed to have been first made against an **Insured** when any **Insured** first receives written notice of such **Claim**.

A **Claim** under any First Party Insuring Agreement of this Policy will be deemed to have been first made when the Company first receives written notice of such **Claim**.

(12) **"Cloud Provider"** means any **Third Party** that provides computing resources to an **Insured** under a written contract with the **Insured** to provide such services, which are delivered as a service over a network or the internet (commonly known as "cloud computing"), including email services, Software as a Service, Platform as a Service and Infrastructure as a Service.

(13) **"Computer Operating System"** means **Computer System** software that manages or administers computer hardware, software resources, or provides common services to run an **Application Program**. **"Computer Operating System"** does not include an **Application Program**.

(14) **"Computer System"** means an interconnected electronic, wireless, web or similar system, including all computer hardware and software, used to process and store **Data** or information in an analogue, digital, electronic or wireless format, including, but not limited to, computer programs, **Data**, operating systems, firmware, servers, media libraries, associated input and output devices, mobile devices, devices that are connected to and controlled by the internet (also known as "smart devices"), networking equipment, websites, extranets, off-line storage facilities (to the extent they hold **Data**) and electronic backup equipment.

(15) **"Coverage Period",** with respect to each **Named Insured**, means the period beginning on such **Named Insured's Enrollment Date** and ending on the earliest of:

(a) 12:01 a.m. on the date that is twelve (12) months after the **Enrollment Date**;

(b) the effective date of cancellation or termination of this Policy, or

(c) the effective date of cancellation or termination of the **Named Insured's** coverage under this Policy.

No **Coverage Period** shall begin before the effective date of the **Master Policy Period**.

(16) **"Covered Bank Account"** means a personal account at a financial or banking institution, including any personal trust or investment account, which is maintained by an **Insured** in the **Insured's** name, or in the name of a legal entity established by an **Insured** or on an **Insured's** behalf to manage the **Insured's** personal assets, from which the **Insured** or an **Account Manager** may request the transfer, payment or delivery of **Money** or **Securities**. **Covered Bank Account** does not include any **Business** account.

(17) **"Cyber Bullying"** means a series of two or more willful and repeated or continuing acts of harassment or intimidation, including embarrassment, humiliation, defamation of character, slander, invasion of privacy or threats of violence, committed by using a computer, telephone, mobile device or another electronic device. **"Cyber Bullying"** methods include, but are not limited to, the use of texting, instant messaging, chat rooms, messages, photos, and other content posted on social networking sites to harass and intimidate.

(18) **"Cyber Bullying Expenses"** means:

(a) reasonable and customary charges for the service of a **Therapist**;

(b) reasonable and necessary childcare or caregiver expenses;

(c) reasonable and necessary expenses to temporarily locate;

(d) if the victim of a **Cyber Bullying Incident** is a **Minor**, reasonable temporary private tutoring expenses, unreimbursed tuition or increase in tuition to relocate the **Minor** to another school; and

(e) reasonable and necessary fees and costs to retain a digital forensic analyst or professional cyber security consultant.

Cyber Bullying Expenses must be incurred by an **Insured** within twelve (12) months after the **Cyber Bullying Incident** is discovered.

(19) **"Cyber Bullying Incident"** means **Cyber Bullying** directed at an **Insured** which causes mental anguish or mental injury, as diagnosed by a **Therapist**.

(20) **"Cyber Extortion Expenses"** means reasonable and necessary costs and expenses, other than **Cyber Extortion Monies**, that an **Insured** incurs as a direct result of a **Cyber Extortion Threat**, including the cost to retain or hire a **Third Party** specializing in IT security to determine the validity and severity of a **Cyber Extortion Threat**.

(21) **"Cyber Extortion Monies"** means **Money**, digital currency of any kind, including bitcoin, or **Other Property** that an **Insured** pays to any person or group reasonably believed to be responsible for a **Cyber Extortion Threat**, to prevent or terminate such **Cyber Extortion Threat**.

(22) **"Cyber Extortion Threat"** means a credible threat or series of related credible threats, including a demand for **Cyber Extortion Monies**, which is directed at an **Insured** to:

(a) steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose or misuse **Private Information** taken from an **Insured** through unauthorized access to, or unauthorized use of, an **Insured Computer System**;

(b) infect an **Insured Computer System** with malicious code or ransomware;

(c) corrupt, damage or destroy an **Insured Computer System**;

(d) restrict or hinder access to an **Insured Computer System**, including the threat of a **Denial of Service Attack**;

(e) perpetrate or carry out a **Phishing Attack**; or

(f) steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose or misuse an **Insured's** confidential or proprietary information or **Personally Identifiable Information**.

A series of continuing, related or repeated **Cyber Extortion Threats**, or multiple **Cyber Extortion Threats** resulting from the same attack, event or incident, will be considered a single **Cyber Extortion Threat** and will be considered to have occurred at the time the first of such **Cyber Extortion Threats** occurred.

(23) **"Cyber Operation"** means the use of a **Computer System** by, at the direction, or under the control of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a **Computer System** of or in another sovereign state.

(24) **"Damages"** means:

(a) a monetary judgment, award or settlement;

(b) awarded attorneys' fees and costs;

(c) prejudgment and post-judgment interest awarded against an **Insured** on that part of any judgment paid or to be paid by the Company; and

(d) liquidated, punitive, exemplary or multiplied **Damages** to the extent insurable under the law pursuant to which this Policy is construed.

"Damages" does not include any **Insured's** future profits or royalties, restitution or disgorgement of any **Insured's** profits; the costs to comply with orders granting injunctive or non-monetary relief, including specific performance, or any agreement to provide such relief; loss of any **Insured's** fees or profits, the return or offset of any **Insured's** fees or charges, or any **Insured's** commissions or royalties provided or contracted to be provided; taxes, fines, penalties or sanctions; contractual liquidated **Damages** that exceed the amount for which the **Insured** would have been liable in the absence of the liquidated **Damages** agreement; any amount which an **Insured** is not financially or legally obligated to pay; disgorgement of any remuneration or financial advantage to which an **Insured** was not legally entitled; settlements negotiated without **Approval**; monetary judgments, awards, settlements or any other amounts which are uninsurable under the law pursuant to which this Policy is construed or any legal fees and costs awarded pursuant to such judgments, awards or settlements.

(25) **"Data"** means any machine-readable information, including, but not limited to, ready-for-use programs, applications, account information, customer information, health and medical information or other electronic information, irrespective of the way it is used and rendered.

(26) **"Defense Costs"** means reasonable and necessary fees incurred with **Approval** and charged by an attorney(s) designated by the Company to defend a **Claim** and all other reasonable and necessary fees, costs and expenses resulting from the defense and appeal of a **Claim**, if incurred by the Company or by an **Insured** with **Approval**. **"Defense Costs"**

does not include any wages or salaries of an **Insured**, or fees, overhead or other charges incurred by or paid to any **Insured** for any time spent in cooperating in the investigation or defense of a **Claim** or a potential **Claim**.

(27) **"Denial of Service Attack"** means an event caused by unauthorized or unexpected interference or a malicious attack, which is intended by the perpetrator to overwhelm the capacity of a **Computer System** by sending an excessive volume of **Data** to such **Computer System** to prevent access to such **Computer System**.

(28) **"Digital Assets"** means **Data** and computer programs that exist in an **Insured Computer System**. **Digital Assets** does not include computer hardware.

(29) **"Digital Assets Loss"** means reasonable and necessary expenses and costs that an **Insured** incurs to replace, recreate or restore **Digital Assets** to the same state and with the same contents immediately before the **Digital Assets** were damaged, destroyed, altered, misused or stolen, including research costs incurred in recreating **Digital Assets** and expenses for materials and machine time. **Digital Assets Loss** will be determined in accordance with this Policy.

(30) **"Enrollment Date"** means, with respect to each **Named Insured**, the effective date on which such **Named Insured** is enrolled for coverage under this Master Policy, as reflected in the enrollment records maintained and verified by the **Policyholder** in accordance with the enrollment procedures agreed to by the **Policyholder** and the Company.

(31) **"Essential Service"** means any service that is essential for the proper operation and maintenance of vital functions of a sovereign state, including, but not limited to, financial services (including services related to financial institutions and associated financial market infrastructure), health services, utility services, emergency services, and/or services that are essential for the proper operation of the food, energy and/or transportation sector.

(32) **"Family Member"** means any of the following persons residing with a **Named Insured**:

(a) the spouse or registered domestic partner of a **Named Insured**;

(b) any **Minor**;

(c) a student enrolled in school full time, as defined by the school, who was a member of a **Named Insured's** household before moving out to attend school, provided the student is under the age of twenty-four (24) and related to the **Named Insured** by blood, marriage or adoption; and

(d) other persons related to a **Named Insured** by blood, marriage or adoption.

(33) **"Financial Fraud"** means:

(a) an intentional, unauthorized and fraudulent written, electronic or telephonic instruction transmitted to a financial institution, directing such institution to debit, transfer, withdraw or disburse **Money** or **Securities** from a **Covered Bank Account**, which instruction purports to have been transmitted by an **Insured** or **Account Manager**, but was in fact fraudulently transmitted by a **Third Party** without the **Insured's** knowledge or consent;

(b) a **Phishing Attack** directed at an **Insured** or **Account Manager** which fraudulently induces the **Insured** or **Account Manager** to transfer, pay or deliver **Money** or **Securities** from a **Covered Bank Account**;

(c) a **Phishing Attack** directed at an **Insured** or **Account Manager** which fraudulently induces the **Insured** or **Account Manager** to transfer, pay or deliver cryptocurrency from an **Insured's** cryptocurrency wallet;

(d) the theft of **Money** or **Securities** from a **Covered Bank Account** or an **Insured's** personal credit cards as a result of a **Hacking Attack**; or

(e) the theft of cryptocurrency from an **Insured's** cryptocurrency wallet as a result of a **Hacking Attack**.

(34) **"Financial Fraud Loss"** means a direct loss of **Money**, **Securities** or cryptocurrency that an **Insured** sustains because of **Financial Fraud**. **"Financial Fraud Loss"** does not include any amounts reimbursed to an **Insured** by any financial or banking institution, or the theft of **Money** or **Securities** from a **Business** account maintained by an **Insured** or **Account Manager**.

(35) **"First Party Insured Event"** means:

(a) with respect to Breach Event Costs Coverage only, a **Security Breach** or **Privacy Breach**;

(b) with respect to Data Recovery Coverage only, a **System Failure**;

(c) with respect to Cyber Extortion Coverage only, a **Cyber Extortion Threat**;

(d) with respect to Cyber Crime Coverage only, a **Financial Fraud**;

(e) with respect to Identity Theft Expenses Coverage only, **Identity Theft**; and

(f) with respect to Cyber Bullying Coverage only, a **Cyber Bullying Incident**.

(36) **"Hacking Attack"** means any of the following directed at or enacted upon an **Insured Computer System**:

(a) unauthorized access to, or unauthorized use of, an **Insured Computer System**, including any such unauthorized access or unauthorized use resulting from the theft of a password from an **Insured Computer System** or from an **Insured**;

(b) a **Denial of Service Attack** against an **Insured Computer System**;

(c) infection of an **Insured Computer System** by malicious code, or the transmission of malicious code from an **Insured Computer System**; or

(d) an **Act of Cyber Terrorism**.

(37) **"Identity Theft"** means the act of knowingly transferring or using, without lawful authority, a means of an **Insured's** personal identity, with the intent to commit a crime, or aid or abet another to commit a crime, including fraudulent use of an **Insured's** personal identity to establish credit accounts, secure loans or enter into contracts. **"Identity Theft"** includes the fraudulent use of an **Insured's** health insurance numbers to file false health insurance claims or to seek medical treatment, prescription drugs or other medical care, but does not include **Business Identity Theft**.

(38) **"Identity Theft Expenses"** means any of the following incurred by an **Insured** solely because of **Identity Theft**:

(a) reasonable and necessary fees of an attorney selected by the **Insured** to:

(i) defend lawsuits brought against the **Insured** by merchants, financial institutions or their collection agencies;

(ii) remove civil judgments wrongly entered against the **Insured** because of **Identity Theft**;

(iii) challenge the accuracy or completeness of information in a consumer credit report;

(iv) release medical records in cases of medical identity fraud;

(v) contest a tax liability wrongfully incurred by the **Insured** because of **Identity Theft**;

(vi) contest the wrongful transfer of ownership of the **Insured's** tangible property; or

(vii) provide the **Insured** with assistance or representation at an audit or hearing before a government agency.

(b) reasonable and customary costs to obtain an **Insured's** credit reports from established credit bureaus. Such credit reports must be dated within twelve (12) months after discovery of the **Identity Theft**. No more than two credit reports may be obtained from any one established credit bureau.

(c) reasonable and customary costs to monitor an **Insured's** credit for up to twenty-four (24) months. Such credit monitoring must begin no later than six (6) months after an **Insured** first discovers the **Identity Theft**.

The **Identity Theft Expenses** payable under paragraph (a) above will be capped at a maximum hourly rate of $400.00.

(39) **"Impacted State"** means a sovereign state where a **Cyber Operation** has had a major detrimental impact on:

(a) the functioning of that sovereign state due to disruption of the availability, integrity or delivery of an **Essential Service** in that sovereign state; and/or

(b) the security or defense of that sovereign state.

(40) **"Inception"** means the earlier of:

(a) a **Named Insured's Enrollment Date**; or

(b) a **Named Insured's** original effective date of Cyber Insurance, which the **Named Insured** obtained as a member of the **Policyholder**, of which this Master Policy is a direct and continuous renewal.

(41) **"Insured"** means:

(a) any **Named Insured**; and

(b) any **Family Member**.

"Insured" does not include the **Policyholder**; no coverage is afforded under this Policy to the **Policyholder**.

(42) **"Insured Computer System"** means:

(a) a **Computer System** that is owned and operated by an **Insured**, or that is leased to and operated by an **Insured**; and

(b) in addition to paragraph (a) above, with respect to Security and Privacy Liability Coverage and Cyber Extortion Coverage only, **Insured Computer System** also includes a **Computer System** operated by an **Outsourced IT Service Provider**, which is used to provide services to an **Insured**, or for processing, maintaining, hosting or storing **Data** for an **Insured**, pursuant to a written contract with such **Insured** to provide such services.

(43) **"Master Policy Period"** means the period from the effective date to the expiration date of this Policy, as set forth in item 4 of the Declarations, or any earlier termination or cancellation date.

(44) **"Minor"** means any person under twenty-one (21) years of age who is residing with a **Named Insured** and is related to the **Named Insured** by blood, marriage, adoption or legal guardianship.

(45) **"Money"** means a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including, but not limited to, currency, coins, bank notes, bullion, travelers' checks, registered checks and **Money** orders held for sale to the public.

(46) **"Named Insured"** means a natural person who, as of such person's **Enrollment Date**, is a customer in good standing with the **Policyholder** and is enrolled for coverage under this Norton Executive Master Policy, as reflected in the enrollment records maintained and verified by the **Policyholder**.

(47) **"Notification Expenses"** means reasonable and necessary legal expenses, forensic investigation expenses, printing costs, and mailing and postage expenses that an **Insured** incurs to notify affected individuals of a **Security Breach** or **Privacy Breach**.

(48) **"Operating System Event"** means a single act of exploitation of, or a series of related, repeated or continuing acts of exploitation of, software vulnerabilities in a **Computer Operating System**, including, but not limited to ransomware, wiper malware, computer worms, and computer viruses, the impact of which is of sufficient intensity, scale or effect to cause a major detrimental impact on the functioning of a sovereign state due to disruption of the availability, delivery, or integrity of an any **Essential Service** in that sovereign state; provided, however, a major detrimental impact on the functioning of a sovereign state shall not result from an attack, or a related series of attacks, solely impacting the **Insured**. For purposes of this definition, the determination of whether an event constitutes a major detrimental impact on the functioning of a sovereign state will rely upon any available evidence such as information from governments, news media, qualified IT forensics firms, computer experts and claims reported to the Company.

(49) **"Other Property"** means any tangible property, other than **Money** or **Securities**, which has intrinsic value.

(50) **"Outsourced IT Service Provider"** means a **Third Party** that provides information technology services to an **Insured**, including but not limited to, hosting, security management, co-location and **Data** storage, under a written contract with such **Insured** to provide such services. **"Outsourced IT Service Provider"** includes any **Cloud Provider**.

(51) **"Personally Identifiable Information"** means information that can be used to determine, distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, including, but not limited to, financial account numbers, security codes, personal identification numbers (PINs), credit and debit card numbers, medical or healthcare information, social security numbers, driver's license numbers, addresses, passwords, and any other non-public information.

(52) **"Phishing Attack"** means the use by a **Third Party** of fraudulent and intentionally misleading telephone calls, emails, texts, instant messages or other electronic communications or malicious websites to impersonate a legitimate or trustworthy contact, organization or person to solicit **Private Information**, **Money** or cryptocurrency.

(53) **"Policyholder"** means the entity specified as such in Item 1 of the Declarations.

(54) **"Privacy Breach"** means any of the following:

(a) the unauthorized collection, disclosure, use, access, destruction or modification of **Private Information**;
(b) the theft of **Private Information**, including the theft of **Private Information** stored on an **Insured's** unsecured **Data** storage or mobile device, such as a smartphone, tablet or laptop;
(c) the surrender of **Private Information** in a **Phishing Attack**;
(d) an infringement or violation of any rights to privacy; or
(e) breach of a person's right of publicity, false light or intrusion upon a person's seclusion.

A series of continuing, related or repeated **Privacy Breaches**, or multiple **Privacy Breaches** resulting from the same attack, event or incident, will be considered a single **Privacy Breach** and will be considered to have occurred at the time the first of such **Privacy Breaches** occurred.

(55) **"Private Information"** means proprietary or confidential information owned by a **Third Party** that is in the care, custody or control of an **Insured**, or is used by an **Insured** with the consent of such **Third Party**, and **Personally Identifiable Information**.

(56) **"Programming Error"** means an error which occurs during the development or encoding of a computer program, software or application and which would, when in operation, result in a malfunction or incorrect operation of a **Computer System**.

(57) **"Property Damage"** means physical injury to, or impairment, destruction or corruption of, any tangible property, including the loss of use thereof. **Data** is not considered tangible property.

(58) **"Related Claims"** means:

(a) two or more **Claims** made against, or involving, any one **Insured**, which have as a common nexus any fact, circumstance, situation, event or cause, or a series of causally connected facts, circumstances, situations, events or causes;

(b) two or more **Claims** made against, or involving, any one **Insured**, which arise from the same or continuing **Security and Privacy Wrongful Act** or **First Party Insured Event**; or

(c) a single **Claim** made against, or involving, multiple **Insureds** who share in a single Limit of Insurance.

(59) **"Related Hacking Attack"** means a **Hacking Attack** with:

(a) the same actor or a coordinated group of actors;

(b) the same **Attack Vector**;

(c) the same vulnerability; or

(d) the common impacted vendor or group of impacted vendors as any other person or entity holding this cyber insurance coverage through the Company.

Related Hacking Attack does not include a **Hacking Attack** which deceives or manipulates any **Insured** to execute subsequent, intervening actions in order to constitute or cause the **Claim.**

(60) **"Securities"** means negotiable or non-negotiable instruments or contracts representing **Money** or **Other Property**. **"Securities"** does not include **Money**.

(61) **"Security and Privacy Wrongful Act"** means any of the following, but only if actually or allegedly committed by an **Insured**:

(a) the failure to prevent or hinder a **Security Breach** which in turn results in a **Privacy Breach**;

(b) the failure to timely disclose a **Security Breach** or **Privacy Breach** affecting **Private Information**;

(c) the failure to prevent the transmission of malicious code or computer virus from an **Insured Computer System** to the **Computer System** of a **Third Party**;

(d) the failure to prevent or hinder participation by an **Insured Computer System** in a **Denial of Service Attack** directed against the internet site or **Computer System** of a **Third Party**; and

(e) infliction of emotional distress or mental anguish, but only if directly resulting from a peril described in paragraphs (a) through (d) above.

(62) **"Security Breach"** means any of the following, whether a specifically targeted attack or a generally distributed attack:

(a) a **Hacking Attack**; or

(b) the theft or loss of an **Insured's** unsecured **Data** storage or mobile device, including any smartphone, tablet or laptop containing **Private Information**.

A series of continuing, related or repeated **Security Breaches**, or multiple **Security Breaches** resulting from a continuing attack, event, incident or failure of computer security, will be considered a single **Security Breach** and will be considered to have occurred at the time the first of such **Security Breaches** occurred.

(63) **"Special Expenses"** means reasonable and necessary costs and expenses that an **Insured** incurs to:

(a) prevent, preserve, minimize, or mitigate any further damage to **Digital Assets**, including the reasonable and necessary fees and expenses of specialists, outside consultants or forensic experts;

(b) preserve critical evidence of any criminal or malicious wrongdoing; or

(c) purchase replacement licenses for computer programs because the copy protection system or access control software was damaged or destroyed by a **System Failure**.

(64) **"System Failure"** means an unplanned outage, interruption, failure, suspension or degradation of service of an **Insured Computer System**, including, but not limited to, any such outage, interruption, failure, suspension or degradation of service caused directly by a **Hacking Attack**, administrative error or **Programming Error**.

(65) **"Therapist"** means a qualified psychologist or other mental health professional who is licensed or certified under the laws of the jurisdiction in which mental health treatment is given to an **Insured** as a victim of a **Cyber Bullying Incident**.

(66) **"Third Party"** means any entity, company, organization or person who does not qualify as an **Insured** under this Policy. However, **"Third Party"** does not include the **Policyholder**.

(67) **"Unauthorized Trading"** means trading, which at the time of the trade, exceeds permitted financial limits or is outside of permitted product lines.

(68) **"War"** means any war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, or confiscation, nationalization, requisition or destruction of or damage to property by or under the order of any government or public or local authority, or any action taken by a government authority to hinder, control, prevent, suppress or defend against any of the aforementioned actions.

(69) **"Widespread Event"** means a **Related Hacking Attack** that impacts 40 other persons holding this cyber insurance coverage through the Company that is discovered, or should have been discovered, within 90 days of the first such person discovering, or when the first such person should have discovered, such **Hacking Attack**.

EXCLUSIONS AS TO THE ENTIRE POLICY

This Policy does not apply to any **Claim**:

(A) made by or on behalf of an **Insured** against another **Insured**.

(B) based upon, arising from or in any way involving any of the following committed by an **Insured**, whether acting alone or in collusion with other persons:

(1) any willful, intentional, deliberate, malicious, fraudulent, dishonest or criminal act or omission;

(2) any intentional violation of law; or

(3) the gaining of any profit or advantage to which an **Insured** is not legally entitled.

However, the Company may pay **Defense Costs** incurred in connection with the defense of any conduct described in this Exclusion until such time as there is a final, non-appealable adjudication in a judicial, administrative or alternative dispute proceeding, or by an **Insured's** own admission in a proceeding or otherwise. The Company will have the right to recover **Defense Costs** incurred in defending any such **Claim** from any **Insured** found to have committed the conduct described in this Exclusion.

(C) based upon, arising from or in any way involving an **Insured's** activities as a stockholder, owner, manager, agent, partner, officer, director or employee of any **Business** or organization, corporation or company.

(D) for **Bodily Injury** or **Property Damage**.

(E) based upon, arising from or in any way involving any of the following, regardless of any other cause or event that contributes concurrently or in any sequence to the **Claim**:

(1) electrical or mechanical failures or interruption, including electrical disturbance, spike, brownout or blackout; or

(2) any regional, countrywide or global outage, failure, disruption or reduction in supply of any utility service or infrastructure, including electricity, gas, water, telephone, cable, internet, satellite or telecommunications, or any failure, outage, disruption, degradation or termination of any critical part of such service or infrastructure.

(F) based upon, arising from or in any way involving the violation of any economic or trade sanctions by the United States government, including, but not limited to, sanctions administered and enforced by the United States Treasury Department's Office of Foreign Assets Control (OFAC). However, this Exclusion does not apply to a **Security Breach** originating from any country where the United States of America has imposed economic or trade sanctions.

(G) based upon, arising from or in any way involving any breach of any express, implied, actual or constructive contract, warranty, guarantee or promise. However, this Exclusion does not apply to:

(1) any liability or obligation an **Insured** would have had in the absence of such contract, warranty, guarantee or promise;

(2) a **Claim** under Security and Privacy Liability Coverage for an unintentional breach by an **Insured** of the provisions of a confidentiality or non-disclosure agreement relating to the confidentiality of **Private Information**.

(H) based upon, arising from or in any way involving any liability assumed by any **Insured** under a contract or agreement. However, this Exclusion does not apply to:

(1) any liability an **Insured** would have had in the absence of such contract or agreement; or

(2) a **Claim** under Security and Privacy Liability Coverage for liability **Assumed Under Contract**.

(I) based upon, arising from or in any way involving:

(1) any actual, alleged or threatened presence of pollutants or contamination of any kind, including, but not limited to, asbestos, smoke, vapor, soot, fumes, acids, alkalis, chemicals and waste ("waste" includes materials to be recycled, reconditioned or reclaimed), whether or not such presence results from an **Insured's** activities or the activities of others, or such presence or contamination happened suddenly or gradually, accidentally or intentionally, or expectedly or unexpectedly; or

(2) any directive or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants, or in any way respond to or assess the effects of pollutants or contamination of any kind.

(J) based upon, arising from or in any way involving income loss caused by or resulting from **Unauthorized Trading**.

(K) based upon, arising from or in any way involving:

(1) the actual or alleged purchase or sale of **Securities**;

(2) the actual or alleged loss of value of any **Securities**;

(3) the offer of, or solicitation of an offer, to purchase or sell **Securities**; or

(4) the violation of any **Securities** law including, but not limited to, the provisions of the Securities Act of 1933, the Securities Exchange Act of 1934 or the Sarbanes-Oxley Act of 2002, or any regulation promulgated under the foregoing statutes, or any similar federal, state, local or foreign law, including "Blue Sky" laws, whether such law is statutory, regulatory or common law.

(L) based upon, arising from or in any way involving the actual or alleged government enforcement of any federal, state, local or foreign regulation, including, but not limited to, regulations promulgated by the United States Federal Trade Commission, the Federal Communications Commission or the Securities and Exchange Commission.

(M) based upon, arising from or in any way involving:

(1) any employer-employee relations, policies, practices, acts or omissions;

(2) any actual or alleged refusal to employ any person; or

(3) any misconduct with respect to employees.

(N) based upon, arising from or in any way involving any actual or alleged harassment or discrimination including, but not limited to, discrimination based on age, color, race, gender, creed, national origin, marital status, sexual preferences, disability or pregnancy.

(O) based upon, arising from or in any way involving:

(1) the violation of any pension, healthcare, welfare, profit sharing, mutual, or investment plan, fund or trust; or

(2) the violation of any provision of the Employee Retirement Income Security Act of 1974 and its amendments, or the Pension Protection Act of 2006 and its amendments, or any regulation, ruling, or order issued pursuant to the foregoing statutes.

(P) for any loss, damage, cost or expense:

(1) directly or indirectly caused by, resulting from or in connection with any **War**;

(2) resulting from a **Cyber Operation** carried out as part of any **War**; or

(3) resulting from a **Cyber Operation** that causes a sovereign state to become an **Impacted State**.

However, this Exclusion does not apply to an **Act of Cyber Terrorism**. Exclusion **(P)**(3) also does not apply to the direct or indirect effect of a **Cyber Operation** on an **Insured Computer System** that is not physically located in an **Impacted State** but is affected by a **Cyber Operation**.

(Q) based upon, arising from or in any way involving any actual or alleged infringement of any patent.

(R) based upon, arising from or in any way involving the misappropriation, theft, copying, display or publication of any trade secret. However, this Exclusion does not apply to a **Claim** under Security and Privacy Liability Coverage for failure to prevent the misappropriation of a trade secret which results from a **Security and Privacy Wrongful Act**.

(S) based upon, arising from or in any way involving the confiscation, commandeering, requisition or destruction of, or damage to, computer hardware by order of a government de jure or de facto, or by any public authority for whatever reason.

(T) for any loss or expense arising from illness, substance abuse or death.

(U) for any loss of cryptocurrency that an **Insured** sustains as a result of:

(1) an outage, interruption, failure, suspension or degradation of service of a **Computer System** owned, controlled, leased or operated by any cryptocurrency wallet provider or cryptocurrency exchange;

(2) the theft of cryptocurrency in a network attack against a **Computer System** owned, controlled, leased or operated by any cryptocurrency wallet provider or cryptocurrency exchange, including a **Denial of Service Attack**, **Act of Cyber Terrorism** or infection of such **Computer System** by malicious code; or

(3) the insolvency or bankruptcy of any cryptocurrency wallet provider or cryptocurrency exchange.

(V) based upon, arising from or in any way involving a **Widespread Event.**

The determination of whether an event constitutes a **Widespread Event** will rely upon any available evidence such as information from governments, news media, qualified IT forensics firms, computer experts and claims reported to the Company.

(W) based upon, arising from or in any way involving:

(1) the theft, misappropriation or misuse of information belonging to, or in the care, custody or control of the **Policyholder** or any of its subsidiaries, partners or affiliates (collectively, "Gen Digital");

(2) a failure or breach of the security intended to protect any **Computer System** that is owned or operated by, or under the control of, Gen Digital, including, but not limited to, that which is caused by unauthorized access, unauthorized use, infection by malicious code or **Denial of Service Attack**;

(3) any outage, interruption, failure, suspension or degradation of service of any **Computer System** that is owned or operated by, or under the control of, Gen Digital; or

(4) any **Security Breach** or **Privacy Breach** caused by or resulting from, in whole or in part, the introduction of malicious code or other vulnerabilities into an **Insured Computer System** by way of insertion of malicious code into any software which is developed, sold or distributed by Gen Digital.

EXCLUSIONS AS TO ALL FIRST PARTY INSURING AGREEMENTS

In addition to the Exclusions as to the entire Policy, the Company will not be liable under any First Party Insuring Agreement of this Policy for:

(A) any liability to any **Third Party** for whatever reason, including contractual penalties, **Damages** or legal costs and expenses of any type.

(B) sanctions, fines or penalties imposed by law.

(C) any **Claim** based upon, arising from or in any way involving fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, force majeure or any other physical event, however caused.

(D) any **Claim** based upon, arising from or in any way involving an **Operating System Event**.

EXCLUSIONS AS TO DATA RECOVERY COVERAGE

In addition to the Exclusions as to the entire Policy, the Company will not be liable under Data Recovery Coverage for:

(A) the cost of restoring, updating or replacing **Digital Assets** to a level beyond that which existed prior to the **System Failure**.

(B) physical damage to, or the costs to repair or replace, any computer hardware or **Data** center.

(C) the economic or market value of **Digital Assets**.

(D) the costs or expenses incurred to identify, patch or remediate software **Programming Errors** or **Computer System** vulnerabilities.

(E) the cost to upgrade, improve, repair, redesign, reconfigure or maintain an **Insured Computer System** to a level of functionality beyond that which existed prior to the **System Failure**.

(F) the cost of restoring, replacing or repairing any electronic media.

EXCLUSIONS AS TO CYBER CRIME COVERAGE

In addition to the Exclusions as to the entire Policy, the Company will not be liable under Cyber Crime Coverage for:

(A) any **Claim** based upon, arising from or in any way involving any actual or alleged unauthorized acquisition, access, use or disclosure of **Private Information** that is held or transmitted in any form. However, this Exclusion does not apply to **Financial Fraud** which directly results from the use of **Private Information**.

(B) amounts that have been wholly or partially reversed by a credit card company or financial institution.

(C) loss of **Other Property** arising out of, resulting from or in any way involving the fraudulent or purportedly fraudulent use of a credit or debit card.

(D) any **Claim** based upon, arising from or in any way involving any fraudulent instruction, if the sender, or any person or organization acting in collusion with the sender, ever had authorized access to an **Insured's** password, PIN or other security code. However, this Exclusion does not apply to **Financial Fraud Loss** resulting from a **Phishing Attack** directed at an **Insured** or **Account Manager** which fraudulently induces the **Insured** or **Account Manager** to (1) transfer, pay or deliver **Money** or **Securities** from a **Covered Bank Account** or (2) transfer, pay or deliver cryptocurrency from an **Insured's** cryptocurrency wallet.

(E) any **Claim** based upon, arising from or in any way involving the giving or surrendering of **Money**, **Securities** or **Other Property** in any exchange for or purchase of goods or services:

(1) that are not yet delivered, whether fraudulent or not;

(2) that fail to conform to advertised quality or performance; or

(3) that fail to conform to the quality or performance expected from the standpoint of the **Insured**.

(F) any **Claim** based upon, arising from, or in any way involving potential income, including interest and dividends, not realized by any **Insured**.

NOTIFICATION

Notice Provisions as to All Insuring Agreements

With respect to all Insuring Agreements of this Policy, an **Insured** must provide written notice to the Company of any **Claim** as soon as practicable during the **Coverage Period**, but no later than sixty (60) days after expiration of the **Coverage Period**.

POLICY CONDITIONS

(A) Assistance and Cooperation

(1) As a condition precedent to coverage under this Policy, every **Insured** shall cooperate with the Company and its representatives and, upon the Company's request, shall submit to examination by a representative of the Company, under oath if required; attend hearings, depositions and trials; assist in effecting settlement; cooperate in the securing and giving of evidence, obtaining the attendance of witnesses, and in the conduct of suits; and shall give a written statement(s) to the Company's representatives for the purpose of investigation and/or defense, all without charge to the Company. Every **Insured** shall further cooperate with the Company to do whatever is necessary to secure and effect any rights of indemnity, contribution or apportionment that any **Insured** may have. No **Insured** shall take any action which in any way increases the Company's exposure under this Policy.

(2) Every **Insured** must execute or cause to be executed all papers and render all assistance as reasonably requested by the Company, which may require an **Insured** to provide copies of a **Third Party's** system security and event logs.

(3) No **Insured** will admit liability, make any payment, assume any obligation, incur any expense, enter into any settlement, stipulate to any judgment or award or dispose of any **Claim** without **Approval**. However, the prompt public admission of a **Privacy Breach** or **Security Breach** potentially impacting the **Private Information** of **Third Parties** will not be considered an admission of liability requiring **Approval**; provided, however, that an **Insured** must provide notice to the Company, in accordance with this Policy, of such public admission, if it is a circumstance that could lead to a **Claim**.

(B) Subrogation

(1) If any payment is made under this Policy, the Company shall be subrogated to the extent of such payment to all rights of recovery thereof, and the **Insured** shall execute all documents required and do everything that may be necessary to secure such rights, including the execution of such documents necessary to enable the Company to effectively bring suit in the name of any **Insured**, and shall provide all other assistance and cooperation which the Company may reasonably require. The **Insured** shall do nothing after a **Claim** is made to prejudice the Company's subrogation rights.

(2) Any recoveries shall be applied first to subrogation expenses, second to **Damages**, **Defense Costs** or any other amounts incurred by the Company, and lastly to the Deductible, if applicable. Any additional amounts recovered will be paid to the **Insured**.

(C) Other Insurance

This Policy is excess over any other valid and collectible insurance (including the amount of any deductibles and/or retentions) available to any **Insured**, including any insurance under which there is a duty to defend and regardless of

whether such other policy or policies are stated to be primary, contributory, excess, contingent or otherwise, unless such insurance is written specifically as excess insurance of this Policy by reference in such other policy to the Policy number set forth in the Declarations of this Policy.

(D) Dispute Resolution

(1) **Mediation**

If any dispute arises between any **Insured** and the Company involving this Policy or a **Claim** hereunder, the **Named Insured** and the Company agree that such dispute will be referred to a qualified mediator in a good faith effort to negotiate a resolution of the dispute prior to the initiation of any arbitration or other proceedings. The party invoking the agreement to mediate will provide written notice to the other party setting forth its request to mediate and a brief statement regarding the issue to be mediated. The **Named Insured** is authorized and directed to accept the Notice of Mediation on behalf of any **Insured**.

(2) **Arbitration**

As a condition precedent to any right of action hereunder, in the event that a good faith effort to mediate pursuant to paragraph (1) above does not resolve a dispute between any **Insured** and the Company involving this Policy or a **Claim**, the **Named Insured** and the Company agree that such dispute will be determined by final and binding arbitration before a single arbitrator. If the parties cannot mutually select the arbitrator, the parties will refer the selection of the arbitrator to the American Arbitration Association.

(E) Policyholder's Rights and Duties

The **Policyholder**, on behalf of all **Insureds**, shall be:

(1) authorized to make changes in the terms of this Policy, with the Company's consent;

(2) authorized to agree to and receive any endorsements issued to form a part of this Policy;

(3) responsible for payment of all premiums; and

(4) responsible for providing any notices to **Insureds** required of the **Policyholder** under this Policy, including notices of cancellation or non-renewal of this Policy or a **Named Insured's** coverage, as applicable.

CURRENCY AND PAYMENTS

All premium and losses under this Policy shall be payable in United States dollars.