

Digital Protection

Operation of cover

Any **insured event** concerning 1st party losses must be first discovered by **you** during the **policy period** and reported to **us** during the **policy period** and up to 72 hours after the termination of the **policy period**.

Any **third party claim** must first be made against **you** during the **policy period** and reported to **us** during the **policy period** and up to 72 hours after the termination of the **policy period**.

Any **insured event** arising from the same original cause will be deemed to be one **insured event**, covered at the time of the first **insured event** of the series, including application of **deductible** and **limit of liability** at that time. This applies to **insured events** discovered during the **policy period** and reported to **us** during the **policy period** and up to 72 hours after the termination of the **policy period**.

What is covered

Subject to the applicable **limit of liability**, **deductible**, conditions and exclusions:

1. Theft of Funds

We will indemnify **you** for any direct and pure financial loss sustained by **you**

- a. as a result of a **theft of funds** due to an unauthorized access to **your** bank account, credit or debit card or **mobile wallets** by a **third party**, and
- b. as a consequence of **you** being a victim of **phishing** or **email spoofing**,

provided that:

- i. **you** report to the issuing bank or the mobile

wallet company within 72 hours after discovery of the **theft of funds**,

- ii. **you** provide evidence that the issuing bank or the mobile wallet company is not reimbursing **you** for the **theft of funds**, and

- iii. **you** lodge a police report detailing the **theft of funds** within 72 hours upon discovery by **you**

- c. **We** will indemnify **you** any reasonable and necessary costs incurred by **you** for prosecution of a criminal case against the **third party** for committing the **theft of funds** or the **phishing** or **email spoofing** against **you**.

2. Identity Theft

- a. **We** will indemnify **you** for any direct and pure financial losses including **lost wages** resulting from an **identity theft**, provided that:

- i. **you** have reported to **us** and the local police within 72 hours after discovery of the **identity theft**, and
- ii. **you** can provide a confirmation from **your** employer that the **lost wages** are not be repaid.

- b. **We** will indemnify **you** for the reasonable and necessary costs incurred by **you** for credit monitoring services and identity monitoring.
- c. **We** will indemnify **you** for any reasonable and necessary costs incurred by **you** for prosecution of a criminal case against a **third party** for committing **identity theft** against **you**.
- d. **We** will pay to or on behalf of **you**, all reasonable fees, costs and expenses of **psychological assistance and treatment** resulting from an **identity theft**.

3. **Data Restoration / Malware Decontamination**

We reimburse **you** for any reasonable and necessary costs incurred by the involvement of an IT **expert** after a **cyber incident** to restore **your data** or to decontaminate or clean **your personal device** from **malware**, to the closest possible condition in which they were immediately before the **cyber incident**.

4. **Cyber Bullying, Cyber Stalking and Loss of Reputation**

- a. **We** will indemnify **you** for any reasonable and necessary costs incurred by **you** for civil proceedings against a **third party** for committing **cyber bullying** or **cyber stalking** against **you**.
- b. In case of an evident and significant **loss of reputation** caused by **cyber bullying** or **cyber stalking**, we will indemnify **you** for any reasonable and necessary costs and expenses for an **expert** to manage and restore **your** reputation.
- c. **We** will indemnify **you** for all reasonable fees, costs and expenses for a necessary relocation of school due to a significant and ongoing **cyber bullying** or **cyber stalking**, provided that the relocation was recommended by an **expert** or relevant authorities.
- d. **We** will indemnify **you** for all reasonable fees, costs and expenses of **psychological assistance and treatment** resulting from **cyber bullying** or **cyber stalking**.

5. **Cyber Extortion.**

We will reimburse **you** for any reasonable and necessary costs to resolve **cyber extortion** as well as any **ransom** **you** pay (where legally permissible and subject to **our** prior written consent).

If so requested by **us**, **you** must notify any relevant law enforcement authorities of the **cyber extortion**.

6. **Online Shopping**

We will reimburse **you** for **your** direct and pure financial loss due to transactions on the internet via payment card or **mobile wallet** that **you** have been dishonestly induced to enter by a **third party** by electronic means to make a purchase of goods or services which are not delivered or rendered; provided that:

- i. **you** can show that **you** have made reasonable attempts to seek a recovery or refund from the **third party** and/or seller of the goods and services to indemnify **you** for **your** financial loss; and
- ii. the fraud event is reported by **you** to **your** card **issuer**, payment service provider or bank or other relevant entity within 48 hours of discovery by **you**; and
- iii. **your** card issuer, payment service provider or bank or other relevant entity refuses in writing to reimburse **you** for transactions made by **you** as a result of the fraud.

7. **Online Sales**

We will reimburse **you** for **your** direct and pure financial loss resulting from you selling non-commercially goods online to a dishonest or fraudulent **third party** buyer, where you have lost physical control of the goods but in return never have received due payment for such goods; provided that **you** can show that **you** have made reasonable attempts to seek payment or recover the delivered goods from the **third party** buyer or other relevant parties to indemnify **you** for **your** financial loss, including involvement of the police.

8. **Social Media and Media Liability**

- a. **We** will pay any sums for which **you** are legally liable arising from a **third party claim** for any unintentional:
 - i. defamation,
 - ii. breach of copyright, title, slogan, trademark, trade name, service mark, service name or domain name, or

iii. breach or interference of privacy rights, resulting from **your online media activities** including media activities in social media.

- b. We will also reimburse **your legal costs** incurred by **you** resulting from the **third party claim** as set forth in **Clause 8.a**.

9. Network Security Liability

- a. We will pay any sums for which **you** are legally liable arising from a **third party claim** for a **cyber incident** on **your personal devices** that **you** failed to prevent and which has caused damage, alteration, destruction or theft of data or a **DoS attack** on **third parties'** computer systems.
- b. We will also reimburse **your legal costs** incurred by **you** resulting from the **third party claim** as set forth in **Clause 9.a**.

10. Privacy Breach and Data Breach Liability

- a. We will pay any sums for which **you** are legally liable arising from a **third party claim** for a **data breach** relating to **confidential information** or **personal data** of a **third party**.
- b. We will also reimburse **your legal costs** incurred by **you** resulting from the **third party claim** as set forth in **Clause 10.a**.

11. Privacy Breach and Data Breach by Third Party

We will reimburse **your legal costs** incurred by **you** for claims for damages filed by **you** against a **third party** for **data breach** relating to your **confidential information** or **personal data**, provided the **third party** has communicated in writing to **you** or has acknowledged publicly by electronic or print media the occurrence of a **data breach** of **your confidential information** or **personal data**.

12. Smart Home Cover

We reimburse **you** for any reasonable and necessary costs incurred by the involvement of an IT **expert** after a **cyber incident** to

decontaminate and restore **your smart home devices**, to the closest possible condition in which they were immediately before the **cyber incident**.

Value Added services

We provide value added services which enhances customer satisfaction such as:

1. Identity Monitoring

- Individual
- Small Business

We provide 24/7 dark web monitoring services which helps stop a data breach from becoming identity theft. It protects Your private credentials which are most frequently exposed in a data breach. If a data breach occurs and your information is exposed, we will send you an alert and give you expert advice and recommendations on what to do for each individual type of personal information.

Features:

- Scanning of email and phone number credentials for exposure in a data breach -
- Details of the breach and recommendations to protection
- Alerts 24/7

2. Cyber education-

- Family & Kids
- Individual

We provide a service which is an effective approach to enhance cyber security awareness.

Integrating videos and interactive content can engage You and will help you to identify the exact requirement

Features:

- Training & education content in local languages
- Written and video content

3. Cyber training-

-SME/Employees

- Business

We have designed a program which will help members to reduce the likelihood of a cyber attack through employee training. The training would comprise of videos and interactive material, as well as refresher modules, which helps in cyber security.

Features include:

- i. Training relevant to each individual's level of cyber awareness.
- ii. Content is concise, relevant, and is provided at regular intervals, saving time for employees while reinforcing key messages.
- iii. The continual nature of the training also helps to combat complacency and ensures that employees are equipped to deal with this ever-changing threat.
- iv. Ability to test comprehension and track employee progress.

Each module finishes with a short test to confirm that the content has been clearly understood.

The progress of all employees can be monitored by administrator. A hassle-free experience. The training is accessible on any device, and with each learning module being short and concise, employees can complete the training at a time and setting that suits them.

Instructional videos provide users and administrators with the information they need to complete their training.

The program features nine learning modules. Subjects include protecting personal information, social engineering attempts, phishing and password safety.

4. Incident Response – Helpline / Online Guided Version

- Individual

- Business

Incident Response is available in 2 formats -

1) Incident Response helpline: From investigation to dealing with a cyber emergency, our Incident Response team

helps resolve all aspects of a digital scam or cyber attack with industry-leading expertise. In the event of a breach, the Incident Response team is your safety net to recover and help restore your family's personal, financial and private information. Our hands-on support helps you get back to normal as quickly and efficiently as possible, and reduce the risk of future compromise.

Features:

Available via phone or email
 Extended business hours, 24/7 in English
 Guided self-assistance solution to compliment human support

2) Incident Response online guided version - It provides an automated support portal to assist You in triaging and responding to cyber incidents. The online support tool will provide a guided user journey to collect relevant details from You and provide instant recommendations on how to respond, in order to protect yourselves. Support includes guidance on coordinating with financial institutions, service providers, and government institutions, as well as how to increase security and monitoring of the accounts. It will help guide You on the actions that You need to take on the most common 'incidents' consumers face.

5. Digital Health Check

- Individual

- Business

We provide service for a customizable risk assessment questionnaire with up to 20 questions as a robust method. It allows for tailored evaluations and provides a comprehensive risk score. Analyzing the results can offer valuable insights and recommendations to address weaknesses and reduce risk exposure.

6. Attack surface Management (ASM)

Features include:

1. Its a platform service, where all internet connected business assets: domains, subdomains, IPs, ports, and services can be monitored continuously for cyber security vulnerabilities and potential attack vectors

2. Easy to understand security score with recommendations on how to improve the security posture of your business.
3. Backed by insurance claims data

7. Wi-fi Scan

- Individual

This service provides you to explore security vulnerabilities and potential threats within your WIFI network, utilizing advanced scanning techniques to identify and address concerns proactively.

Features:

- Scan your WiFi network for any threats
- Provide advanced detections of wireless network attacks through spoofing, and SSL stripping & splitting.

8. Safe Browsing

- Individual

This service helps you to safeguard your online experience, by shielding you from websites that could compromise your privacy. By steering clear of harmful sites, it enhances both security and privacy.

9. Endpoint Protection (iOS & Android)

- Individual

Your mobile device is fortified with cutting-edge security standards and features, ensuring it remains free from potentially unwanted programs. It's optimized with the latest security settings and fortified with antivirus and anti-malware protection for robust defense.

Note that some features will vary according to the device type (iOS or Android).

Features-

- System scan for devices, end point protection & security configuration
- Device cleaning & optimisation (Android)
- Anti-virus & anti-malware protection (Android)

What is not covered

We will not cover any claim by **you** under this **policy** arising directly or indirectly from the following:

1. **insured events** or circumstances that could reasonably lead to an **insured event** which are known by **you** prior to the inception of this **policy**.
2. any action or omission of **you** or any misbehaviour of **you** which is intentional, malicious, dishonest, deliberate or reckless;
3. any action or omission in **your** capacity as employee or self-employed person as well as any professional or business activity.
4. any type of war (whether declared or not), use of force or hostile act.
5. loss of or damage to tangible property and any consequential losses resulting therefrom, including the loss of use of tangible property.
6. investment or trading losses including without limitation any inability to sell, transfer or otherwise dispose of securities.
7. bodily injury, psychological harm (save that this exclusion shall not apply to anxiety or mental stress as set forth in **Section 2 – Identity Theft and Section 4 – Cyber Bullying, Cyber Stalking and Loss of Reputation**), trauma, illness or death.
8. misappropriation, theft, infringement, or disclosure of any intellectual property (such as patents, trademarks, copyrights). This exclusion shall not apply to **Section 8 – Social Media and Media Liability**. However, theft, infringement, misuse or abuse of patents will always remain excluded.
9. **third party claims** made by one **insured** against another **insured**.
10. contractual liability which exceeds legal liability which would otherwise arise.
11. any costs of betterment of **your personal device** or **your smart home devices** beyond the state existing prior to the **insured event**, unless unavoidable.

12. Any type of cryptocurrencies (e.g. Bitcoin, Ethereum, Ripple, IOTA).. This exclusion shall not apply to **Section 5 – Cyber Extortion** with regards to any **ransom** payments.
13. Gambling.
14. Failure, interruption, degradation or outage of infrastructure or related services of the following third party providers :
telecommunication, internet service, satellite, cable, electricity, gas or water providers

How to make a claim

1. **Reporting.** You must report as soon as is reasonably practicable to **us** or to the **incident response provider** any actual **insured event**. which may give rise to payment under this **policy**.
2. **Assistance and Cooperation.** You shall:
 - a. cooperate with **us** or the **incident response provider** including preserving any **hardware, software** and **data**,
 - b. provide all documents and information and render all assistance as reasonably requested by **us** or the **incident response provider**, and
 - c. assist in the conduct of suits, in making settlements, and in enforcing any right of contribution or indemnity against any person or organization that may be liable to **you** because of acts, errors, or omissions covered under this **policy**.
3. **Claims against you.** You must not, without **our** prior written consent, admit liability for, pay, settle or prejudice any **third party claim**. You must assist **us** in investigating, defending and settling the **third party claim**, and assist any lawyer or other **expert we** appoint on **your** behalf to defend the **third party claim**. You must pay the **deductible** to any **third party we** require to comply with any settlement.
If **we** have directly indemnified any **third**

party, you must immediately reimburse **us** for the amount of the applicable **deductible**.

4. Basic documents to be submitted by insured for claim settlement (To be submitted by insured after reporting of loss)

1. Incident Report: Detailed description of the cyber incident, including when and how it occurred.
2. Evidence of Breach: Logs, screenshots, and any other evidence of the breach or attack.
3. Insurance Policy Documents: A copy of the cyber liability insurance policy.
4. Notification of Breach: Any notifications sent to affected individuals or regulatory bodies.
5. Incident Response Plan: Documentation of the steps taken to mitigate the breach.
6. Legal Notices: Any legal notices or communications related to the breach.
7. Financial Loss Documentation: Evidence of financial losses incurred due to the incident, including invoices, financial statements, or loss calculations.
8. Forensic Report: If applicable, a report from a cybersecurity firm detailing the breach's scope and impact.
9. Communication Records: Records of communications with stakeholders, including customers and partners, about the breach.
10. Restoration Costs: Documentation of costs incurred for restoring systems and data.

Escalation Matrix

Level 1 - contactclaims@universalsompo.com

Level 2 - grievance@universalsompo.com

Level 3 - gro@universalsompo.com

General conditions

1. **Our liability.** We will not be liable for the **deductible** applicable to each and every **insured event** or **third party claim**. Our liability will be in excess of any **deductible** and subject to the **limit of liability** for each and every **insured event** or **third party claim** as stated in the **schedule**.
2. **Representation and Warranty.** In issuing this **policy** we have relied upon **your** statements, representations and information as being true and accurate. If your statements, representations or information contain misrepresentations which were made with the actual intent to deceive and which materially affect **our** acceptance of the risk or the hazard assumed, **we** shall not be liable for a loss or claim based upon, arising from, or in consequence of, any such misrepresentation.
3. **Preconditions.** We are only obliged to indemnify **you** in accordance with this **policy** if **you**:
 - a. make sure **your personal devices** or **smart home devices** are used and maintained as recommended by the manufacturer or supplier, and
 - b. prevent and mitigate loss or damages covered under this **policy** by:
 - i. Providing, maintaining and updating the operational system of **your personal devices and smart home devices** within 14 days after a security patch was advised to be installed,
 - ii. Deployment of appropriate system, device and data security measures (e.g. anti-malware solutions),
 - iii. Usage of appropriate passwords, and
 - iv. Maintaining and updating at appropriate intervals backups of **your data**, at least every 14 days.
4. **Payment under more than one section.** Any cover affecting more than one section of cover will be subject to the highest applicable **deductible**.

5. **Renewal:** We agree to renew the policy on payment of the renewal premium. However, we retain our right not to renew the policy on any ground, more particularly of fraud, misrepresentation or suppression of any material fact either at the time of taking the policy or any time during the currency of the earlier policies or bad moral hazard
6. **Subrogation.** If any payment is made under this **policy**, **we** will be subrogated to the extent of such payment up to all **your** rights of recovery from any **third party**. **You** must do all that is necessary to secure and must not prejudice such rights. Any monies recovered will be applied first to any costs and expenses made to obtain the recovery, second to any payments made by **us**, and third to any other payments made by **you**.
7. **Other Insurance.** If there is other insurance for the same **insured event** this **policy** will apply in excess of this other policy and will not contribute with this other insurance.
8. **Cancellation.**

This Policy will terminate at the expiration of the period for which premium has been paid or on the expiration date shown in the Policy Schedule

You may cancel this Policy at any time by sending fifteen (15) days notice in writing to **Us** or by returning the Policy and stating when thereafter cancellation is to take effect. In the event of such cancellation **We** will retain the premium for the period that this Policy has been in force and calculated in accordance with

the short period rate table, provided that there is no claim under this Policy during the **Period of Insurance**

We reserve the right to cancel this Policy from inception immediately upon becoming aware of any mis-representation, mis-declaration, fraud and/or, nondisclosure of material facts and /or non-cooperation by

You or on **Your** behalf. No refund of premium shall be allowed in such cases Notice of cancellation will be mailed to **You** at **Your last known** address as set forth in the Policy

Schedule, and will indicate the date on which coverage is terminated. If notice of cancellation is mailed, proof of mailing will be sufficient proof of notice given to you. In case of any claim under this Policy or any of its individual coverage in such an event no refund of premium shall be allowed

Period the Policy has run	Policy Premium to be Retained
Not Exceeding 1 Month	25% of the Annual premium
Not Exceeding 2 Months	35% of the Annual premium
Not Exceeding 3 Months	50% of the Annual premium
Not Exceeding 4 Months	60% of the Annual premium
Not Exceeding 6 Months	75% of the Annual premium
Not Exceeding 8 Months	85% of the Annual premium
Exceeding 8 Months	Full Annual Premium

The grounds for cancellation of the policy, for the insurer, can be only on the grounds of misrepresentation, non-disclosure of material facts, fraud or non-co-operation of the insured.

9. Premium Payment: The premium has to be received by us in full on or before the policy inception date. In the event of non-realisation of the premium, the Policy shall be treated as void-ab-initio.

10. Notices: Notices must be in writing and sent by e-mail, registered post or hand to the addresses stated in the **schedule** or any other agreed addresses. **You** may give notice by telephone but must send a written notice as soon as practical afterwards.

11. Assignment. **You** must not assign any legal rights or interests in this **policy** without **our** prior written consent.

12. Variations. Variations to this **policy** must be agreed by the **named insured** and **us** in writing.

13. Laws or regulations. If any provision of this **policy** conflicts with the laws or regulations of

any jurisdiction in which this **policy** applies, this **policy** must be amended by the **named insured** and **us** to comply with such laws or regulations.

14. Severability. Any unenforceable provision of this **policy** will not affect any other provisions and, if practicable, will be replaced with an enforceable provision with the same or similar intent as that unenforceable provision.

15. Third party rights. No **third party** who is not a party to this **policy** shall have any right to enforce any part of this **policy**.

16. Law and jurisdiction. This **policy** will be governed by the laws as stated in the **schedule**. The courts as stated in the **schedule** will have exclusive jurisdiction for any dispute.

17. Arbitration. The parties to the contract may mutually agree and enter into a separate Arbitration Agreement to settle any and all disputes in relation to this policy. Arbitration shall be conducted under and in accordance with the provisions of the Arbitration and Conciliation Act, 1996.

18. Definitions. A definition in this **policy** to the singular shall include the plural and vice versa.

Definitions

Aggregate limit of liability – the amount stated in the **schedule** which shall be the maximum amount payable by **us** under this **policy** whether in respect of first party cover or **third party claims** or payment of any expenses including any payment made by **us** to the **incident response provider**.

Confidential information – any form of sensitive information not publicly available, whether or not marked as 'confidential'.

Cyberbullying – any acts of:

- harassment (including foster personal interaction repeatedly despite a clear indication of disinterest)

- b) intimidation,
 - c) defamation of character,
 - d) illegitimate invasion of privacy (including monitoring the use of the internet, email or any other form of electronic communication); or
 - e) threats of violence,
- committed against **you** over the internet.

Cyber extortion – any credible and unlawful threat or series of threats by a **third party** extortionist against **you** with the intention to cause harm or damage to **your data** on **your personal device** or **your personal device** in order to extract a extortion ransom from **you** by use of coercion.

Cyber incident – any **malicious act** or **malware** occurring on **your personal devices** or **your smart home devices**.

Cyber Stalking – means the repeated use of electronic communications to harass or frighten someone.

Data – any digital information, irrespective of the way it is used, stored or displayed (such as text, figures, images, video, recordings or **software**).

Data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, **personal data** or **confidential information** transmitted, stored or otherwise processed on **your personal devices**.

Deductible – each **deductible** as stated in the **schedule**, being the amount which **you** must incur before this **policy** responds.

DoS attack – any **malicious act** causing total or partial disruption or unavailability of **personal devices** or **smart home devices** by an overloading stream of requests, including distributed denial-of-service attacks.

Email spoofing – any forgery or wrongful manipulation of an email so that the the receiver of such a message is misleading to believe that

Digital Protection : UIN: IRDAN134CP0045V01202324

the email is real and therefore trusts the faked origin of the message.

Expert – any person or legal entity appointed by or in consultation with **us** and/or the **incident response provider** (such as an IT, lawyer or public relations consultant).

Hardware – the physical components of any **personal devices** used to store, record, transmit, process, read, amend or control **data**.

Identity theft – the theft of **personal data** over the internet, which has resulted or could reasonably result in the wrongful use of such **personal data**.

Incident response provider – the legal entity stated in the **schedule**.

Insured – means:

- a) the **named insured** as set forth in the **schedule**; and
- b) any **listed family members** of the **named insured** as additional **insureds** as set forth in the **schedule**.

Insured event – any **theft of funds**, **cyber incident affecting your personal devices**, **identity theft**, **cyberbullying**, **cyber stalking**, **cyber extortion**, financial loss due to **online sale** or **online shopping**, cyber incident affecting **your smart home devices** and **third-party claim**.

Legal costs – any costs, expenses and/or fees for **experts**, investigations, court appearances, surveys, examination and/or procedures that are necessary for **your** civil, administrative and/or criminal proceedings. This does not include **your** general expenses (such as salaries and overheads).

Limits of liability – as stated in the **schedule**, including any sub-limit and aggregate limit of liability.

Loss of reputation – any adverse effect on **your** reputation due to a publication on the internet by a **third party**.

Lost wages – any salary that was lost or not paid by **your** employer, solely as a result of any **insured event**. Computation of lost wages for self-employed persons must be supported by, and will be based on, prior year tax returns.

Malicious act – any unauthorised or illegal act of a **third party** intending to cause harm to or to gain access to, or disclose **data** from **personal devices** or **smart home devices** through the use of any **personal device**, **smart home device**, computer system or computer network including the internet.

Malware – any unauthorised or illegal **software** or code (such as viruses, spyware, computer worms, trojan horses, rootkits, ransomware, keyloggers, dialers and rogue security **software**) designed to cause harm to or to gain access to or disrupt **personal devices** or **smart home devices** or computer networks.

Mobile wallet – means any online account in which **you** deposit or earn money which is denominated in a specific currency that can be spent in a (online) store.

Online media activities – any text, images, videos or sound distributed via **your** website, social media presence or e-mail.

Personal data – any information relating to a data subject who can be identified, directly or indirectly, in relation to other information (such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person) as defined by applicable data protection laws.

Personal devices – any devices (computers, laptops, tablets, mobile phones, etc.) used for the purpose of creating, accessing, processing,

protecting, monitoring, storing, retrieving, displaying or transmitting **data**. The term personal devices shall not encompass any **smart home devices**.

Phishing – the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication, but does not include any verbal forms of electronic communication.

Policy – the **schedule** and **policy**.

Policy period – the duration of this **policy** as stated in the **schedule**.

Premium – the amount payable by **you** as stated in the **schedule**.

Psychological assistance and treatment – the involvement of an accredited psychiatrist, psychologist or counsellor chosen by **you** at **your** own discretion with the prior written consent of **us**, not to be unreasonable withheld or delayed, to treat **you** for stress, anxiety or such similar medical conditions.

Ransom – any money, bitcoins or other digital currency demanded by a **third party** in the course of a **cyber extortion**.

Smart home devices – any devices or IoT components used by **you** in **your** household in order to operate or control smart home enabled devices such as cameras, air conditioning, lighting, alarming systems or fire protection systems.

Software – any digital standard, customised or individual developed program, or application held or run by a **personal device** that comprises a set of instructions that are capable, when incorporated in a machine readable medium, of causing a machine with information processing capabilities to indicate, perform or achieve a particular function, task or result.

Theft of funds – any unauthorized electronic transfer of money, assets or any other funds.

Third party – any person or legal entity other than the **insured** as stated in the **schedule**.

Third party claim – any written demand or assertion for compensation or damages by a **third party** against **you**.

We, us and **our** – the **insurer** or their agent as stated in the **schedule**.

You and **your** – the **insured**.

Your personal devices – any **personal devices** owned, leased or licensed, and directly controlled by **you**.

CONTACT US

Contact Us for Queries, Requests and Suggestions

In case you have any queries kindly contact us on our 24*7 toll free Nos: 1800 - 22- 4030 or 1800-200-4030

Senior Citizen: Toll free: 1800 267 4030.

You can also email your queries on Email : contactus@universalsompo.com

In case you need further assistance regarding the query resolution, kindly follow the grievance process as mentioned below

GRIEVANCES

If You have a grievance about any matter relating to the Policy, or Our decision on any matter, or the claim, You can address Your grievance as follows:

➤ Step 1

a. Contact Us

1-800-224030/1-800-2004030

b. E-mail Address:

Contactus@universalsompo.com

c. Write to us Customer Service Universal Sampo General Insurance Company Limited

Unit No. 601 & 602, 6th Floor, Reliable Tech Park, Thane- Belapur Road, Airoli, Navi Mumbai, Maharashtra - 400708

d. Senior Citizen Number: 1800 267 4030

➤ Step 2

If the resolution you received, does not meet your expectations, you can directly write to our Grievance Id. After examining the matter, the final response would be conveyed within two weeks from the date of receipt of your complaint on this email id.

Email Us- grievance@universalsompo.com

Drop in Your concern

Grievance Cell: Universal Sampo General Insurance Co. Ltd, Unit No. 601 & 602, 6th Floor, Reliable Tech Park, Thane- Belapur Road, Airoli, Navi Mumbai, Maharashtra - 400708

Visit Branch Grievance Redressal Officer (GRO)
Walk into any of our nearest branches and request to meet the GRO

- We will acknowledge receipt of your concern immediately
- Within 2 weeks of receiving your grievance, we will respond to you with the best solution.
- We shall regard the complaint as closed if we do not receive a reply within 8 weeks from the date of our response

➤ Step 3

In case, You are not satisfied with the decision/resolution of the above office or have not received any response within 15 working days, You may write or email to:

Chief Grievance Redressal Officer

Universal Sampo General Insurance Company Limited

Unit No. 601 & 602, 6th Floor, Reliable Tech Park, Thane- Belapur Road, Airoli, Navi Mumbai, Maharashtra - 400708

Email : gro@universalsompo.com

For updated details of grievance officer, kindly refer the link

<https://www.universalsompo.com/resource-grievance-redressal>

➤ Step 4

Bima Bharosa Portal link :

<https://bimabharosa.irdai.gov.in/>

Insurance Ombudsman

You can approach the Insurance Ombudsman depending on the nature of grievance and financial implication, if any. Information about Insurance Ombudsmen, their jurisdiction and powers is available on the website of the Insurance Regulatory and Development Authority of India (IRDAI) at www.irdai.gov.in, or of the General Insurance Council at <https://www.gicouncil.in/>, the Consumer Education Website of the IRDAI at <http://www.policyholder.gov.in>, or from any of Our Offices.

The updated contact details of the Insurance Ombudsman offices can be referred by clicking on the Insurance ombudsman official site: <https://www.cioins.co.in/Ombudsman>

Note: Grievance may also be lodged at IRDAI <https://bimabharosa.irdai.gov.in/>

The contact details of the Insurance Ombudsman offices are as below-

Office Details	Jurisdiction of Office Union Territory, District)
AHMEDABAD Office of the Insurance Ombudsman, Jeevan Prakash Building, 6th floor, Tilak Marg, Relief Road, Ahmedabad – 380 001.	Gujarat, Dadra & Nagar Haveli, Daman and Diu.

Tel.: 079 - 25501201/02/05/06 Email: bimalokpal.ahmedabad@cioins.co.in	
BENGALURU - Office of the Insurance Ombudsman, Jeevan Soudha Building, PID No. 57-27-N-19 Ground Floor, 19/19, 24th Main Road, JP Nagar, 1st Phase, Bengaluru – 560 078. Tel.: 080 - 26652048 / 26652049 Email: bimalokpal.bengaluru@cioins.co.in	Karnataka
BHOPAL Office of the Insurance Ombudsman, 1st floor, "Jeevan Shikha", 60-B, Hoshangabad Road, Opp. Gayatri Mandir, Bhopal – 462 011. Tel.: 0755 - 2769201 / 2769202 Email: bimalokpal.bhopal@cioins.co.in	Madhya Pradesh Chattisgarh.
BHUBANESHWAR Office of the Insurance Ombudsman, 62, Forest park, Bhubaneswar – 751 009. Tel.: 0674 - 2596461 / 2596455 Fax: 0674 - 2596429 Email: bimalokpal.bhubaneswar@cioins.co.in	Odisha
CHANDIGARH Office of the Insurance Ombudsman,	Punjab, Haryana(excluding Gurugram, Faridabad,

S.C.O. No. 101, 102 & 103, 2nd Floor Batra Building, Sector 17 – D, Chandigarh – 160 017 Tel.: 0172 - 4646394 / 2706468 Email: bimalokpal.chandigarh@cioins.co.in	Sonepat and Bahadurgarh) Himachal Pradesh, Union Territories of Jammu & Kashmir, Ladakh & Chandigarh.
CHENNAI Office of the Insurance Ombudsman, Fatima Akhtar Court, 4th Floor, 453, Anna Salai, Teynampet, CHENNAI – 600 018. Tel.: 044 - 24333668 / 24333678 Email: bimalokpal.chennai@cioins.co.in	Tamil Nadu, Puducherry Town and Karaikal (which are part of Puducherry).
DELHI Office of the Insurance Ombudsman, 2/2 A, Universal Insurance Building, Asaf Ali Road, New Delhi – 110 002. Tel.: 011 – 23237539 Email: bimalokpal.delhi@cioins.co.in	Delhi & Following Districts of Haryana - Gurugram, Faridabad , Sonepat & Bahadurgarh
GUWAHATI Office of the Insurance Ombudsman, Jeevan Nivesh, 5th Floor, Nr. Panbazar over bridge, S.S. Road, Guwahati – 781001(ASSAM). Tel.: 0361 - 2632204 / 2602205 Email: bimalokpal.guwahati@cioins.co.in	Assam, Meghalaya, Manipur, Mizoram, Arunachal Pradesh, Nagaland and Tripura.
HYDERABAD	Andhra Pradesh,

Office of the Insurance Ombudsman, 6-2-46, 1st floor, "Moin Court", Lane Opp. Saleem Function Palace, A. C. Guards, Lakdi-Ka-Pool, Hyderabad - 500 004. Tel.: 040 – 23312122 Email: bimalokpal.hyderabad@cioins.co.in	Telangana, Yanam and part of Union Territory of Puducherry.
ERNAKULAM Office of the Insurance Ombudsman, 10th Floor, Jeevan Prakash, LIC Building, Opp to Maharaja's College, M.G.Road, Kochi - 682 011. Tel.: 0484 - 2358759 Email: bimalokpal.ernakulam@cioins.co.in	Kerala, Lakshadweep, Mahe- a part of Union Territory of Puducherry
KOLKATA Office of the Insurance Ombudsman, Hindustan Bldg. Annexe, 7th Floor, 4, C.R. Avenue, KOLKATA - 700 072. Tel.: 033 - 22124339 / 22124341 Email: bimalokpal.kolkata@cioins.co.in	West Bengal, Sikkim, Andaman & Nicobar Islands.
LUCKNOW Office of the Insurance Ombudsman, 6th Floor, Jeevan Bhawan, Phase-II, Nawal Kishore Road, Hazratganj, Lucknow - 226 001. Tel.: 0522 - 4002082/3500613 Email:	Districts of Uttar Pradesh : Lalitpur, Jhansi, Mahoba, Hamirpur, Banda, Chitrakoot, Allahabad, Mirzapur, Sonbhadra, Fatehpur, Pratapgarh, Jaunpur, Varanasi, Gazipur, Jalaun, Kanpur, Lucknow,

bimalokpal.lucknow@cioins.co.in	Unnao, Sitapur, Lakhimpur, Bahraich, Barabanki, Raebareli, Sravasti, Gonda, Faizabad, Amethi, Kaushambi, Balrampur, Basti, Ambedkarnagar, Sultanpur, Maharajgang, Santkabirnagar, Azamgarh, Kushinagar, Gorkhpur, Deoria, Mau, Ghazipur, Chandauli, Ballia, Sidharathnagar.
MUMBAI Office of the Insurance Ombudsman, 3rd Floor, Jeevan Seva Annexe, S. V. Road, Santacruz (W), Mumbai - 400 054. Tel.: 69038800/27/29/31/32/33 Email: bimalokpal.mumbai@cioins.co.in	Goa, Mumbai Metropolitan Region excluding Navi Mumbai & Thane.
NOIDA Office of the Insurance Ombudsman, Bhagwan Sahai Palace 4th Floor, Main Road, Naya Bans, Sector 15, Distt: Gautam Buddh Nagar, U.P-201301. Tel.: 0120-2514252 / 2514253 Email: bimalokpal.noida@cioins.co.in	State of Uttaranchal and the following Districts of Uttar Pradesh: Agra, Aligarh, Bagpat, Bareilly, Bijnor, Budaun, Bulandshehar, Etah, Kanooj, Mainpuri, Mathura, Meerut, Moradabad, Muzaffarnagar, Oraiyya, Pilibhit, Etawah, Farrukhabad, Firozbad, Gautambodhanagar, Ghaziabad, Hardoi,

	Shahjahanpur, Hapur, Shamli, Rampur, Kashganj, Sambhal, Amroha, Hathras, Kanshiramnagar, Saharanpur.
PATNA Office of the Insurance Ombudsman, 2nd Floor, Lalit Bhawan, Bailey Road, Patna 800 001. Tel.: 0612-2547068 Email: bimalokpal.patna@cioins.co.in	Bihar, Jharkhand.
PUNE Office of the Insurance Ombudsman, Jeevan Darshan Bldg., 3rd Floor, C.T.S. No.s. 195 to 198, N.C. Kelkar Road, Narayan Peth, Pune – 411 030. Tel.: 020-24471175 Email: bimalokpal.pune@cioins.co.in	Maharashtra, Area of Navi Mumbai and Thane excluding Mumbai Metropolitan Region.

REGISTERED & CORP OFFICE:

**Universal Sampo General Insurance Company
Limited:**

**8th Floor & 9th Floor (South Side), Commerz
International Business Park, Oberoi Garden
City, Off Western Express Highway, Goregaon
East, Mumbai 400063.**

Contact US:

24/7 Customer Care: Toll free Nos: 1800 - 22-
4030 or 1800-200-4030

Email: contactus@universalsampo.com

Website: www.universalsampo.com

IRDAI Registration Number:134

CIN: U66010MH2007PLC166770