

Cyber Complete Insurance

Summary of Cover

This is a summary of our Cyber Complete insurance policy and does not contain the full terms and conditions of the cover, which can be found in the policy document. It is important that you read the policy document carefully when you receive it. Your cover depends on the choices you have made. Your policy schedule document will show the items you have chosen to cover along with the cover limits.

What is Cyber Complete Insurance?

Aviva cyber insurance protects you against loss of, or damage to, information from IT systems and networks. It covers such things as hackers and cyber criminals causing damage or disruption to data, the subsequent loss of profit and funds as well as your liability arising from an event. It gives you 24/7 access to an incident manager and the specialist support required to recover from a cyber related event.

Cyber Incident Response

Cover for the costs of responding to a cyber incident that directly affects your business or an outsourced service provider.

Cover includes:

- ✓ **Crisis Management** - 24/7 access to Cyber Incident Crisis Manager.
- ✓ **IT Investigation and Forensic Costs** - cost of IT forensic experts for cause identification and incident containment.
- ✓ **Legal and Regulatory Management** - costs to manage legal response, breach notifications and regulatory and law-enforcement reporting.
- ✓ **Communications Costs** - costs of PR consultants to minimise adverse publicity following an incident.
- ✓ **Privacy Breach Management Costs** - costs for notifying affected individuals, credit or identity fraud monitoring services and helpline support.
- ✓ **Extortion Resolution Costs** - cost of specialist negotiation support and recovery costs or ransom payment (where insurable by law).
- ✓ **Criminal Reward Fund** - reward cost to help identify offenders or recover losses, where legally permissible.
- ✓ **Resilience Improvement** - cost to improve resilience of computer systems following a claim.

Significant **exclusions and limitations**

- ✗ We will only reimburse extortion or reward payments if they are deemed legally permissible.
- ✗ We will not cover prior claims or circumstances that you were aware of, or ought to have known of, prior to the cover start date.
- ✗ We will not cover any proceedings or claims brought by a subsidiary, parent or associate company.

Computer and Data Rectification

Cover for reinstating or restoring data, removing viruses or malware and replacing damaged computer hardware.

Cover includes:

- ✓ **Data Restoration Costs** – cost of restoring data following virus, hacking or denial of service attack and removing virus or similar mechanism.
- ✓ **Hardware Replacement (Bricking) Costs** – cost to repair or replace damaged computer equipment.

Significant exclusions and limitations

- X We will not cover replacement of industrial control systems or operational technology (OT) equipment.
- X We will not provide betterment, except for where original versions are unavailable.

Business Interruption

Cover for loss of profit and increased costs of working as a result of a cyber incident or system failure directly affecting your computer equipment or the computer equipment of an outsourced service provider.

Cover includes:

- ✓ **Loss of Profit** – Loss of profit caused by a cyber incident, including loss from a necessary voluntary and intentional shutdown.
- ✓ **Increased Costs of Working (ICOW)** – costs for reasonable expenditure incurred to reduce or avoid a loss of profit.
- ✓ **Additional Increased Costs of Working (AICOW)** – costs for additional expenditure incurred to reduce or avoid a loss of profit.
- ✓ **System Failure** – Loss of profit caused by an unplanned outage of your own systems due to software, hardware or network failure, or human error.
- ✓ **Outsourced Service Provider (OSP) Failure** – Loss of profit and ICOW following a cyber incident or system failure of an OSP's computer systems.
- ✓ **Consequential Reputational Harm** – Loss of profit caused by the loss of a current or future customer as a direct result of a cyber incident or system failure.

Significant exclusions and limitations

- X Outages causing interruption less than the Waiting Period.
- X Property damage – loss, destruction of or damage to property
- X Failure of infrastructure, including satellite provider, utility provider, internet service provider, telecommunications provider, domain name service, certificate authority or content delivery network.

Cyber Crime

Cover for financial loss resulting from cyber enabled theft, fraud or unauthorised system use.

Cover includes:

- ✓ **Funds Transfer Fraud** - loss of funds following fraudulent electronic instruction moving money from your account without consent, or following a third party deceiving an employee into paying or transferring money by impersonating another person.
- ✓ **Theft of Personal Money** - loss of personal funds from directors' or employees' personal bank accounts resulting from unauthorised access.
- ✓ **Telephone Hacking** - charges incurred due to unauthorised access to your telecommunication system.
- ✓ **Unauthorised Use of Computer Equipment** - costs following unauthorised use of your computer systems by a third-party for crypto-mining, hacking or denial-of-service attacks.

Significant exclusions and limitations

- X Losses involving fraud or collusion by the insured.
- X Losses caused by intentional or dishonest acts by directors or partners.

Online Risk and Reputation

Cover for support and costs incurred to manage online impersonation, fraud, misinformation and deepfake attacks.

Cover includes:

- ✓ **Corporate Identity Fraud** - costs to correct or reinstate public records, defend legal proceedings, and investigate the perpetrator.
- ✓ **Online Risk Response** - access to reputation protection services and legal fees for online impersonation, misinformation and similar online attacks.
- ✓ **Targeted Deepfake Attack** - support to identify and remove deepfake content and manage reputational impact, including platform monitoring and crisis management.

Significant exclusions and limitations

- X Prior claims or circumstances that you were aware of, or ought to have known of, prior to the cover start date.
- X Proceedings or claims brought by a subsidiary, parent or associate company.

Network Security and Privacy Liability

Cover for liability resulting from data breaches, security failures and regulatory or payment card industry (PCI) related claims.

Cover includes:

- ✓ **Network Security Liability** – transmission of a virus or unauthorised access resulting in a Denial-of-Service attack or access to data.
- ✓ **Privacy and Confidentiality Liability** – including unauthorised disclosure of personal, or confidential commercial, data; breach of confidence or failure to notify data subjects.
- ✓ **Payment Card Industry Liability** – costs of forensic investigation, recertification, non-compliance fees, and card re-issuance following a payment card data breach.
- ✓ **Regulatory Fines and Penalties** – legal defence costs and any lawfully insurance regulatory fines and penalties following Data Protection Regulations breach from a cyber incident.

Significant exclusions and limitations

- X Contractual liability unless specifically part of PCI requirements.
- X Fines and Penalties which are not legally insurable.
- X Loss or liability resulting from unlawful surveillance or unsolicited communications.

Multimedia Liability

Legal protection for online content risks such as defamation or copyright infringement.

Cover includes:

- ✓ **Defamation** – legal liability for defamation of character, libel or slander caused by your business media.
- ✓ **Intellectual Property Infringement** – plagiarism or infringement of trademarks, registered designs, or copyright in connection with the business.
- ✓ **Media Removal Costs** – costs to remove online content to prevent or mitigate a claim.

Significant exclusions and limitations

- X Patent infringement and trade secret misappropriation.
- X Future business losses such as future value of licenses or royalties.
- X Any liability arising from the provision of, or failure to provide, professional services or professional advice or a breach of any contract for the provision of professional services or professional advice.

Additional Benefits

- **Cyber Incident Response**

24/7 access to a Cyber Incident Crisis Manager via a dedicated hotline, providing expert advice, consultancy and coordination of the full cyber incident response, including online reputation and deepfake crisis support.

- **24 hour, 365 days a year claims helpline - providing emergency assistance when it's needed**
- **Counselling service** - for you as a policyholder and your employees
- **Aviva Risk Management Solutions - <https://www.aviva.co.uk/risksolutions>**

Aviva Risk Management Solutions (ARMS) is a dedicated service to help UK businesses manage their risks - helping to keep them compliant, prevent loss and ultimately control cost.

ARMS offer a wide range of training and consultancy services from simple loss prevention advice through to bespoke on-site consultancy and offer generous discounts off a menu of products and services to help prevent accidents and losses occurring and protect businesses via our Specialist Partner Network.

- **Aviva BusinessLaw - <https://avivabusinesslaw.farill.io/>**

This is a complimentary website, provided by Aviva, offering many tools and resources to help your client manage their business effectively, including unlimited legal advice via the legal advice helpline, business and legal guides, document builders etc. that can help with the day-to-day running of the business, as well as helping to manage exposure to legal risk.

What are my obligations?

This is a summary of your main obligations under the policy.

- You must make a fair presentation of the risk to us, which includes telling us of any circumstances which we would take into account in our assessment or acceptance of this insurance. If you fail to make a fair presentation of risk this could affect the extent of cover provided or invalidate your policy.
- You must also make a fair presentation to us in connection with any variations, e.g. changes you wish to make to your policy.
- You must take all reasonable precautions to prevent loss or damage, and comply with any security or other loss prevention conditions in your policy documents.
- You must notify us promptly of any event which might lead to a claim and follow the claims procedure set out in your policy.
- For further details and any specific obligations relating to your trade or business activities following our assessment of your risk, please refer to your policy documents.

How long does my Aviva Business Insurance run for?

Your policy will remain in force for 12 months from the date of commencement (or as otherwise shown on your Schedule) and for any period for which you renew the policy, as long as you continue to pay your premium.

How to Claim

Claims can be reported via our cyber claims team on **0800 051 4473**.

Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.

How do I make a complaint?

If for any reason you are unhappy with the product or service, please get in touch as soon as possible. For contact details and more information about the complaints procedure please refer to your policy documents.

Where a complaint cannot be resolved to your satisfaction you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights. You can contact the FOS on **0800 023 4567** or visit their website at **www.financial-ombudsman.org.uk**, where you will find further information.

Where am I covered?

This will depend on the product and choices you have made. Please refer to the policy booklet for details of where you are covered.

When and how do I pay?

Payment options should be discussed with your insurance adviser.

How do I cancel the contract?

You can cancel your policy at any time during your period of cover, subject to the notice period shown in your policy. To cancel, contact your insurance adviser.

Would I receive compensation if Aviva were unable to meet its liabilities?

Depending on the circumstances of your claim you may be entitled to compensation from the Financial Services Compensation Scheme (FSCS) if we cannot meet our obligations. **See [fscs.org.uk](https://www.fscs.org.uk)**

Telephone Call Charges and Recording

Calls to 0800 numbers from UK landlines and mobiles are free. The cost of calls to 02 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Risks situated within the UK and other countries excluding the EEA are underwritten by Aviva Insurance Limited. Registered in Scotland, No. SC002116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 202153.

Risks situated within the EEA are underwritten by Aviva Insurance Ireland Designated Activity Company. Aviva Insurance Ireland Designated Activity Company, trading as Aviva, is regulated by the Central Bank of Ireland.

Firm Reference Number C171485. A private company limited by shares. Registered in Ireland, No. 605769. Registered Office: Cherrywood Business Park, Dublin, Ireland, D18 W2P5. Registered UK Branch Address: 80 Fenchurch Street, London, EC3M 4AE. UK Branch authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority (Firm Reference Number 827591) and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request.