CYBERSOS®
:RESPOND

YOUR SERVICE PLAN

The CYBERSOS:RESPOND cyber emergency service

Contents

THE CYBERSOS:RESPOND SERVICE PLAN

TERMS AND CONDITIONS

This service is designed to help **you** in case **your devices** suffer a **cyber attack**, you lose access to **your personal data**, or if **your online identity** is stolen, compromised or publicly maligned online.

These terms and conditions set out **our** and **your** responsibilities in relation to the **service plan**.

DEFINITIONS

We use certain words throughout this document that have a specific meaning and they are shown in bold. These are called 'definitions' and their meaning can be found below:

Cyber attack	Malicious or unauthorised access by a **third party** to a **device** or **online service** that results in: - the deletion, corruption or theft of **personal data**; - damage to or corruption of the **device** itself; - a **device** being rendered inaccessible or unusable either temporarily (e.g. in the case of ransomware) or permanently (e.g. via other **malware** including viruses)
Device	A computer, laptop, mobile telephone or tablet owned by **you**, and used primarily for **your** personal, non-professional, non-commercial means: A **device** can not be a **smart home device**.
Device personal data	**Personal data** stored on a **device**.
Home	**Your** main place of residence in the United Kingdom.
Incident	An event that prompts **you** to contact **us** either by phone or online requesting the help provided by this **service plan**.
Malware	Software or code maliciously designed by a **third party** to disrupt, damage or gain access to **your device**.

Online identity	The online representation of **your** personal, individual identity including, but not limited to: - social media profiles; - personal financial profiles, data and information; - real-world identification data and documents; - other **online services**.
Online personal data	**Personal data** held by a digital, electronic service or membership that requires **you** to log-in via online authentication e.g. an email address and password or mobile phone number.
Online service	A commercially-available third party service for **your** personal, non-professional use accessed by **you** via online authentication e.g. an email address and password or mobile phone number and which contains **personal data**.
Personal data	Electronic data, documents and photographs that are unique to **you** personally and not primarily related to **your** business or employment.
Service plan	This contract for remote, telephone-based cyber emergency support services.
Service plan anniversary	Each 12-month anniversary of the **start date**.
Service plan period	In the first year, this runs from the **start date** to the **service plan anniversary**. In subsequent years, this period runs from one **service plan anniversary** to the next.
Smart home device	The broadband router used to connect **your home** to the internet and other electronic equipment that is primarily designed to be used, managed or monitored via a software application or website and is: - permanently located within **your home**; and - primarily connected to the internet via **your home** broadband network; - not a **device**.
Start date	As confirmed to **you** by **your** Police Federation.
Third party	Anyone other than **you**.
We/us/our	CYBERSOS, a trading style of Vivo Lifestyle Services Ltd, a company registered in England & Wales, Company No 10729223, or our specialist cyber emergency service providers, as appointed from time-to-time.

Working order	The working condition a **device** was in immediately prior to the **incident**.
You/your	The person who has purchased this **service plan** (being the **planholder**), the **planholder's** married or civil partner, children and parents, who all permanently live with the **planholder** at **home**. Children up to the age of 22 who are studying away at college or university in England, Northern Ireland, Scotland or Wales during term time and who return to the **home** during holidays will for the purposes of this **service plan** be treated as permanent residents of the **home**. Anyone eligible to use the **service plan** must have the **planholder's** consent to do so.

WHAT DOES THIS SERVICE PLAN PROVIDE?

This **service plan** provides remote, phone-based emergency support in the event that **you** become the victim of a **cyber attack** or suspected **cyber attack** as described in these terms and conditions. It is designed to help restore **your devices** to **working order**, re-establish access to **your personal data** and restore **your online identity** to the state it was in prior to the **incident**.

You may use this **service plan** for up to 5 hours per **incident**, for up to 2 **incidents** in any **service plan period**.

This service is provided remotely at all times. If **we** are unable to resolve the issue remotely, **we** will generally be able to advise **you** as to what next steps to take, but any action **you** take outside this **service plan** will be at **your** own cost and liability.

!

What devices are eligible for this plan?

Your device must be:

- purchased as brand new directly from the manufacturer, network provider or retail store (high street or online), or
- purchased as used or refurbished directly from the manufacturer or network provider
  and
- used primarily for personal, non-professional, non-commercial purposes.

You must also be able to produce original proof of purchase.

Your device cannot be:

- used or refurbished purchased from either a high street or online retail store i.e. not from the manufacturer or network provider.
- in the case of mobile telephones, those that are outside the manufacturer's stated security update and support period for the specific device when first buying this **service plan**,
- in the case of all other devices, more than 60 months (5 years old) when first buying this **service plan**,
- hardware that has had its original operating system intentionally modified or over-written by **you** such that it does not operate as the manufacturer intended – a process commonly referred to as "jail-breaking", "chipping", "modding" or "cracking".

Is this plan right for you?

You must be 18 years old or over and resident in the United Kingdom to be eligible.

Incidents that occur while **you** and/or **your devices** are outside the United Kingdom are not eligible under this **service plan**.

Your responsibilities

- All information **you** give must be true, factual and not misleading.
- **You** must pay the fees for the **service plan** when they fall due.
- **Devices** must have been used only in accordance with the manufacturer's instructions.
- If **you** suspect a **device** has been compromised by a **cyber attack**, **you** must contact **us** as soon as reasonably possible and take all reasonable steps to limit damage, e.g. stop using the **device** if it is likely to cause further damage or loss of **personal data**, until **you** have done so.
- **You** must co-operate with **us** and provide all information needed by **us** to help **us** resolve **your** issue.

ON-GOING CYBER EMERGENCY HELP AND ASSISTANCE

If you would like to read-up on how you can easily help protect yourself from cyber attacks and generally protect your personal data and online security better, please go to btp.cybersos247.co.uk

SECTION 1 – 24/7 CYBER EMERGENCY HELPLINE

If **you** know or genuinely suspect that one of **your devices** or **your personal data** has been affected by a **cyber attack**, or **your online identity** has been stolen, compromised or publicly maligned by a **third party**, **you** can call one of **our** plain-English speaking cyber experts 24 hours a day, 365 days a year on the Cyber Emergency Helpline number below:

0333 370 1529

We will take time to listen to what is worrying **you** and to understand **your** individual level of comfort and experience of a subject that is unknown and frightening to many.

We will generally be able to help with an initial assessment of the **cyber attack**, loss of **personal data** or attack on **your online identity** and recommend the immediate action **you** should take.

We will also be able to suggest which authorities it is in **your** best interests to notify and how to approach financial institutions such as **your** bank or credit reference agencies, where appropriate.

If one of **your devices** has either stopped working properly or completely, **we** will also be able to give **you** advice on how to restore it to **working order** as well as ways of making it more resistant to attack in the future.

Finally, if **you** wish, **we** can also help **you** take easy steps to better data and personal online security to help safeguard **your** personal information more securely.

Your responsibilities

You must call the helpline as soon as reasonably possible after discovering or suspecting that **you** have been affected by a **cyber attack**, and in all cases within 12 hours of **you** becoming aware of it.

SECTION 2 – CYBER ATTACK ASSISTANCE – DEVICE AND PERSONAL DATA

If a **device** or **personal data** has or appears to have been affected by a **cyber attack**, **we** will work with **you** remotely to:

- establish what the issue is and its cause;
- if identified, attempt to remove any **malware** and check to see if that has resolved the issue;
- if the issue persists, look at other ways to restore **your device** to **working order** or restore access to **your personal data** as efficiently as possible;
- discuss, in the case of ransomware that **we** are unable to bypass or remove successfully from the **device**, what **your** next best steps are. Note: this never results in suggesting the payment of a ransom.

PERSONAL DATA – RE-ESTABLISHING ACCESS OR RESTORATION

Sometimes, the only solution to restore a **device** to **working order** is to wipe it clean of its operating system and all data, and attempt to reinstall them. **We** will help **you** to do that remotely, step-by-step, if **you** wish.

Where **your device personal data** is backed-up elsewhere – physically (on another disk drive) or in the cloud (online) – **you** might accept completely wiping the **device** as the best outcome as **you** will have a clean, **working order device** that **you**, with **our** help if necessary, can restore **your device personal data** to.

However, where no back-up of **device personal data** exists, **we** will discuss **your** priorities with **you** i.e. whether **you** would prefer a restored **device** but risk losing **device personal data**, or whether the **device personal data** is the most important element to restore or protect.

For **online personal data**, **we** will attempt to restore **your** access to it and suggest potential ways of either making it more secure or creating offline backups so that if it should be compromised again, **you** will have more than one source to retrieve it from.

Restoration of devices or personal data

No guarantee
Despite our best efforts, it is not always possible to restore **devices** to **working order**, nor to restore **personal data** or protect it from further harm, and **we** make no guarantee that **we** will do so.

We will explain this clearly to **you** at the outset and throughout **our** work on **your incident**.

Although this service should help **you** mitigate the effects of a **cyber attack**, we cannot guarantee that **your personal data** and **online identity** will not be harmed and, in the absence of any negligence or other breach of duty by **us** (or the partners **we** work with to provide the support), **we** (and they) are not responsible for any theft, damage, destruction or loss suffered by **you** as a result of a **cyber attack**.

Downloading software at our request
In the process of attempting to restore a **device** to **working order**, **we** may ask **you** to download either **our** own proprietary software, or software of trusted third party providers e.g. antivirus software. If **you** decide that **you** are uncomfortable with downloading software **you** are unfamiliar with, it may mean that **we** are unable to provide the full extent of the services **we** would otherwise have been able to offer, and it might compromise a successful outcome. In such cases, **we** will advise **you** how best to proceed in good faith, but the service will end and this **incident** will be closed on **our** system.

SECTION 3 – ACTIVALERT BREACH AND DARK WEB MONITORING

This **service plan** entitles the **planholder** (only) to complimentary access to the ACTIVALERT identity breach and dark web monitoring service.

In order to take advantage of this service, **you** must have acted upon the instructions contained in **your** welcome email from **your** Police Federation. Please be aware that activation needs to be completed in accordance with the instructions in that email for **you** to receive the benefit of the service.

The features of the service are as follows:

ACTIVALERT continuously watches for signs that **your** personal information has been exposed or stolen. By logging in, **you** can see all monitored identifiers in one place and review any alerts relating to **your** personal data.

Alerts provided as part of the service
Alerts will be provided by email and/or SMS, depending on **your** notification settings.

Dark web monitoring
ACTIVALERT scans dark web sources - hidden parts of the internet used by criminals to buy and sell stolen data - for **your** personal details. If **your** information is found in a data breach or criminal marketplace, **you'll** receive an alert by email and/or text message, so **you** can take action quickly. Alerts are sent as soon as a match is detected.

Surface web monitoring
In addition to the dark web, ACTIVALERT also monitors publicly accessible websites and online sources where exposed personal data can appear. This broader coverage means **you're** protected across a wider range of places where **your** information could surface without **your** knowledge.

Botnet and malware alerts
If **your** device credentials - such as usernames, passwords or session data - appear in information harvested by malicious software or botnets, ACTIVALERT will alert **you**. This type of exposure often goes unnoticed, so early warning gives **you** the best chance to secure **your** accounts before any harm is done.

Multiple identifiers monitored
ACTIVALERT can monitor a range of **your** personal details, including email addresses, phone numbers, passwords, date of birth, national insurance number, passport number, driving licence number, bank account details and more. The more identifiers **you** add, the broader **your** protection. *Please note: even though only one individual can sign up for the ACTIVALERT service, many multiples of personal details can be added, which is more than enough to give reassurance across the majority of families.*

Your privacy is protected
ACTIVALERT is built with **your** privacy at its core. **Your** personal details are coded and protected before they ever leave **your** device - meaning the service can alert

you to a match without ever storing **your** sensitive information in readable form. This privacy-first approach is built into the foundations of the service.

Hand-in-hand with CYBERSOS - 24/7 human support
If **you** receive an alert or have any concerns about **your** data security, CYBERSOS specialists are available around the clock, every day of the year. Whether **you** need help understanding an alert, want guidance on what steps to take, or find yourself dealing with the aftermath of fraud or identity theft, a real person is always just a call away - ready to advise, assist and act on **your** behalf. *Please note: **our** specialists do not have access to **your** breach alerts, so **you** will need to give them as much information as **you** are comfortable with in order that they can help **you** as much as possible.*

Expert fraud recovery support
If **you** become a victim of fraud or identity theft, your CYBERSOS team will help guide **you** through every step of the recovery process. This includes help with how to liaise with key organisations, advising on protective measures such as Cifas Protective Registration, and helping **you** put additional safeguards in place to protect **your** identity going forward.

GENERAL CONDITIONS OF THE SERVICE

DURATION AND RENEWAL OF YOUR SERVICE PLAN

Your service plan starts on the date advised to you by **your** Police Federation.

The **service plan** then continues until **your** Police Federation cancels it (unless ended otherwise in accordance with these terms and conditions).

Shortly before each **service plan anniversary**, **your** Police Federation will confirm that the **service plan** has been renewed.

We reserve the right not to offer **you** continuation of **your service plan** at each **service plan anniversary,** but **we** will contact **you** beforehand if **we** intend to do so.

General exclusions

The following are excluded from the **service plan**:

- Physical damage of any kind to any **device**.
- Replacement, recall or modification of a **device** (or any part) by a supplier or the manufacturer.
- Any problem with the supply of electricity or broadband.
- Costs, incidental costs or loss arising from not being able to use a **device**.
- **Cyber attacks**, loss of **personal data** or damage to **your online identity** caused wilfully or deliberately by **you**.
- Any loss occurring outside the **service plan period**.
- Damage to the **online identity** of anyone aged under 18.
- Any loss, damage or impairment to functionality of a **device** caused by neglect.
- Any loss, damage or impairment to functionality of a **device** caused by:
  earthquake, flood, lightning, fire, wind, humidity, weather conditions, salt spray, storm or other natural events or catastrophes, abnormally high or low temperatures, electromagnetic pulse, nuclear material or radioactive contamination, chemical exposure, explosion, sabotage, terrorism, insurrection, revolution, war, riot, armed conflict, civil commotion, rebellion, man-made events or catastrophes.
- Repairs or modifications to a **device** not approved by the **device** manufacturer.
- Damage arising as a result of **you** installing apps or software to a **device** that have not:
  - been purchased or downloaded via a recognised commercial retailer, or
  - been purchased or downloaded via the officially-recognised app or software store of the **device's** operating system provider.
- Loss of pornographic or illegal content or any unlicensed, pirated software, music or films.
- The cost of replacing any **device** consumables or accessories.

Special exclusions

In addition to the 'General exclusions' above, the **service plan** does not provide care for the following:

- Normal operation, updates, upgrades or adjustment of **devices**.

PAYING YOUR FEES

If **you** do not pay for **your service plan** on time, it will be suspended from the due date. No services will be provided past this date unless payment is received.

CANCELLATION AND ENDING OF THE PLAN

Please speak to **your** Federation Office.

OUR RIGHT TO CANCEL YOUR PLAN OR BRING IT TO AN END

If **we** have reasonable grounds to suspect that **your** behaviour is in any way dishonest, exaggerated, fraudulent or obstructive to the efficient carrying out of the services then **we** may cancel the **service plan** immediately without any refund of fee (see 'Fraudulent activity' below).

We may cancel this **service plan** where there is a valid reason for doing so by giving **you** at least 7 days' written notice. Valid reasons include but are not limited to the following:

- where **you** fail to comply with certain conditions (see 'Your responsibilities' above);
- where **you** fail to pay for the **service plan**, if applicable (see 'Paying your fees' above);
- where **you** have (or anyone acting for **you** has) previously engaged in fraudulent activity and/or provided **us** with false information (see 'Fraudulent activity' below); or
- where **you** have used threatening or abusive behaviour or language towards **our** staff or suppliers.

CUSTOMER SERVICES DETAILS

For customer services: get in touch by clicking on 'contact us' on **our** website: https://service.vivolifestyleservices.co.uk/customer-service/

HOW TO COMPLAIN

If **you** wish to complain or **you** are unhappy with the service provided, please contact **our** customer services team (see 'Customer services details' above).

We will attempt to resolve **your** complaint as quickly, professionally and comprehensively to **your** satisfaction as possible. **We** would ask **you** to grant **us** reasonable time to do so.

If **we** are unable to meet **your** reasonable expectations, **we** will issue **you** with a 'final response' to **your** complaint.

If, at that stage, **you** are still not satisfied with how **we** have responded, **you** can approach the Citizens Advice Consumer Service on 0345 404 0506. For more specific advice depending on where **you** live in the UK, please visit https://www.citizensadvice.org.uk/

CHANGES TO THESE TERMS AND CONDITIONS

We may modify or replace these terms and conditions in order to:

- comply with the law, regulations, industry guidance or codes of practice;
- rectify errors or ambiguities; and
- reflect changes in the scope or nature of the services provided to **you**.

We will give **you** thirty (30) days' written notice of any change that could affect **your** rights or obligations and provide **you** with a brief explanation of such changes. The new terms and conditions will take effect from the date specified in the notice. If **you** do not agree with the changes, **you** may cancel the plan within that notice period and, provided that **you** are up-to-date with the payment of fees, **your service plan** will be cancelled immediately.

DATA PROTECTION INFORMATION

Vivo Lifestyle Services Ltd.
This is a brief summary of how **we** protect and respect **your** privacy in accordance with data protection legislation. For more information go to https://vivolifestyleservices.co.uk

HOW DO WE USE YOUR DATA?

We use the data **we** hold about **you** in order to provide **your** cyber emergency service or let **you** know about information, products or services that interest **you**, or for analytical or statistical purposes. **We** also use it to safeguard against fraud and money laundering.

DO WE SHARE YOUR DATA?

By default **we** do not share **your** data other than in the natural course of providing **your service plan** i.e. with **our** helpline experts. At **your** option, **you** can allow **us** to share **your** data more broadly but **we** will always ask **you** first and **you** always have the right to change **your** mind by notifying **us** at https://service.vivolifestyleservices.co.uk/customer-service/

WHAT HAPPENS WITH INTERNATIONAL DATA TRANSFERS?

We may transfer **your** data to countries (including the United States of America) which may not have data protection laws which provide the same level of protection as provided in the UK. However, **we** have safeguards in place to help ensure that everything is adequately secured and protected.

WHAT ARE YOUR RIGHTS?

You have the right to ask **us** to:

- not use **your** data for marketing purposes
- send **you** a copy of the personal information **we** have about **you**
- delete **your** data (subject to certain exemptions)
- correct or delete any inaccurate or misleading data
- restrict the processing of **your** data
- provide a copy of **your** data to any controller
- lodge a complaint with the local data protection authority

HOW LONG DO WE KEEP YOUR DATA?

We won't keep **your** information for any longer than is necessary. In most cases that's 6 years (the reasonable expectation of average **device** lifecycle), or 6 years following the expiry of a **service plan**.

ANY OTHER QUESTIONS?

Please use the online contact form at https://service.vivolifestyleservices.co.uk/customer-service/ and choose the "I have a question about the data you hold on me" option.

EXCLUSION OF THIRD PARTY RIGHTS

No rights or benefits will be given to any other third party under the **service plan**.

FRAUDULENT ACTIVITY

We may provide **your** details to third parties in order to detect possible fraudulent activity.

If **we** have reasonable grounds to suspect that **you** have (or anyone acting for **you** has):

- previously engaged in fraudulent activity; or
- provided **us** with false information,

we may immediately cancel **your service plan** and/or reject an application for new plans.

If **we** suspect that **you** have (or anyone acting for **you** has) engaged in fraudulent activity or provided **us** with false information **we** may request extra information in support of **your** application or request for services (such as a bank or credit card statement to prove ownership).

If **we** have reasonable grounds to suspect that **you** have (or anyone acting for **you** has) requested services under this **service plan** knowing the request to be dishonest, exaggerated or fraudulent, then **we** may:

- request extra evidence in support of **your** request (such as a bank or credit card statement to prove ownership);
- decline **your** request and immediately cancel **your service plan** without any refund of fee paid;
- recover from **you** the cost of any services already provided to **you** under this **service plan** and the cost of any investigation into a fraudulent request under this **service plan** (and **we** may initiate legal proceedings to do so);
- report **you** to the relevant authorities, including the police.

GOVERNING LAW AND STATUTORY RIGHTS

We will communicate with **you** in English and English Law will apply unless **we** agree otherwise with **you**. Nothing in these terms and conditions will reduce or affect **your** statutory rights; for further information about **your** statutory rights contact the Citizens Advice Bureau: www.adviceguide.org.uk or 03454 04 05 06.

COMPANY INFORMATION

This service plan is provided by Vivo Lifestyle Services Ltd, a company incorporated under the laws of England and Wales with Company Registration Number: 10729223.