IT Security Protocol Policy

JUST 1 SOURCE & SUPPLY LTD take IT security very seriously, as it is an integral part of the business.
Whilst every precaution is taken to protect our hardware and software systems, we are fully aware that “cyber-attacks” are becoming ever more regular and more sophisticated.

Therefore, we cover this by having multi delivery networks with independent software platforms. Meaning any “cyber-attack” on one particular network will minimise interruption in continuation of service. We simply switch all despatches to another one of our networks within a couple of hours.

Backing up data
JUST 1 SOURCE & SUPPLY LTD data is backed up with a set backup policy. Each change made to files is backed up to local NAS devices, then uploaded to cloud storage (environment (powered by Acronis). NAS devices are also set to take bare metal backups of all server infrastructure to enable our IT provider a seamless restoration should the worst happen. To avoid redundancy from our customers perspectives, we avoid an "eggs-in-one-basket" scenario by routing delivery traffic via multiple providers (Openfleet, TPN Connect, Mandata, Sterling, Paragon). We are confident should one operator/network, be affected by an issue (virus infection, etc), that we would be able to maintain service for our customer base with minor hassle and inconvenience.

Malware protection
JUST 1 SOURCE & SUPPLY LTD day-to-day security consists of ensuring all machines run supported operating systems and have updates and anti-virus software installed as standard. (Avast, https://www.avast.com/en-gb/business/products/business- antivirus). This is installed automatically and monitored centrally, with any errors picked up promptly and addressed as necessary. Applicable updates are automatic and logged by IT department. Staff are restricted as to what websites apps they can access and all downloads must be approved by our IT division.

Device security
All IT hardware is loaded with the Malware protection and regular updates applied by log monitored by the IT division. The new server operates Microsoft's latest Server 2019 operating system, with zero machines in the environment running out of date / insecure operating systems. The IT replacement program will ensure all devices are up to date and compliant. Additionally, we control how USB drives and memory cards can be used when transferring files between devices or applications. This reduces the likelihood of infection by blocking access to physical ports, using anti-virus tools and only allowing approved drives and cards to be used within the organisation. All smartphones and tablets are password / PIN protected. Tracking is also applied to these devices and we have the ability to lock or wipe where appropriate. Updates are applied to these as per our protocol. We do not allow unknown Wi-Fi hotspots to be used.

Firewall
Firewalls create a buffer zone between our network and external networks (such as the internet). From a server/Internet perspective, we use an enterprise-grade router/firewall across our sites (pfSense, https://www.pfsense.org), which includes additional features over a standard business router to bring extra security to our systems. Two examples are 1) the "pfBlockerNG", used to block "malvertising" and other unsuitable content, and
2) "Snort" (https://www.snort.org) which constantly analyses Internet traffic to detect and stop dangerous or suspicious activity.

Password protection
Passwords are used for every device and software program used by JUST 1 SOURCE & SUPPLY LTD. We have minimum length and differing character passwords that are encrypted employing two-factor authentication (also known as 2FA). This means two different methods to “prove” identity before staff can use a device or software. Further, these are set to enforce change at minimum set periods and deleted should a staff member leave the business.

Phishing awareness
We configure all accounts in advance using the principle of least privilege to reduce the chance of successful phishing attacks. This allows staff to perform the tasks, but minimises potential damage of an attack. Administrator rights are protected and only available to Director level staff. Utilising the 2FA on important accounts further reduces an attacker accessing accounts even if they know one password. As part of our security protocol, we regularly (through our IT support company) do vulnerability/penetration testing and have a dedicated email address to send suspicious emails to be authorised. This includes running a suite of tools and looking for vulnerabilities on our systems such as firewall issues, viruses, out of date firmware/software running on the various devices on our network. All staff are encouraged to report any possible attack and ONLY if they have spoken in person to a Senior member of staff, are they allowed to process any payment and not on the authority of an incoming email purported to be from that person.

Telephone Networks
JUST 1 SOURCE & SUPPLY LTD operate a VOIP-based phone system. This has an advantage over the older ISDN-based system, as we can ensure continuity of phone service should that be required. Using our VOIP system, we can quickly source and configure phone equipment to work from anywhere in the world using our own regular phone numbers.

GDPR - Privacy
Since the inception of the Data Protection Act 2018, all of the above is integral to keeping all data secure. Our separate JUST 1 SOURCE & SUPPLY LTD GDPR Privacy policy is available on request. JUST 1 SOURCE & SUPPLY LTD work alongside a DPO (Data Protection Officer) who works with our IT Provider, ensuring SAR’s are dealt with appropriately and in compliance with all GDPR policies.

Contingency Planning
While we are aware good security is important, we also remain realistic that with whatever security there is in place, it's always possible that can be by- passed by a malicious actor; either targeting our business directly or indirectly. In the case of an entire site failure (for example, fire/flooding, etc), JUST 1 SOURCE & SUPPLY LTD now operate from multi sites, with spare IT capacity available in each. Should the need arise to move staff elsewhere and continue unhindered. If a site becomes unavailable for any reason, we are confident in picking up the operation from elsewhere in hours, ensuring business continuity.

All staff (where applicable) have access to work remotely on JUST 1 SOURCE & SUPPLY LTD networks, so again, should the worst occur, we can still access accounts data / shipping data and anything else required.

Remote teams' access via VPN as all sites have VPN capability which allows staff to connect remotely and securely.

Cyber Insurance Cover
JUST 1 SOURCE & SUPPLY LTD have a comprehensive Cyber Insurance Cover in place. This includes "Incident Response Costs" ensuring we can get immediate assistance in any event of a Cyber-Attack. Details of cover can be provided on request.

References: Information and advice is following from the National Cyber Security Centre www.ncsc.gov.uk

Signed:  Date: **01/01/2025**

Graham Murray

Managing Director - Just 1 Source & Supply Ltd