Statement of Compliance with GDPR

1. SYS3 Limited

SYS3 Limited is a limited company registered in England under the number 04154104

2. Commitment to Information Security

As a business, SYS3 takes data security and privacy extremely seriously. We process personal information on behalf of our customers and we also control the personal information of our own workforce. We are providing you with this Statement of Compliance with GDPR to help you fulfil your own duties as a data controller in respect of supplier due diligence.

3. Information Security Management

SYS3 manages information security in-house in order to control its information assets and the information assets of it's clients correctly.

3.1. Policies & Protocols

	Employees	Contractors
Company Handbook	✓	
Telecoms, IT, Internet & Email	✓	
Data Protection	✓	✓
Information Security Incident Report Form	✓	✓

The above documents provide clarity in respect of:

- Confidentiality
- Clear screen policy
- Monitoring of communications
- Remote working
- Data disposal
- Data breach reporting

SYS3 Limited's relevant policies and protocols help us to fully realise our commitment to **lawful, fair and transparent** data processing.

3.2. Guidelines & Training

SYS3 Limited commits to oversee the competence of all our human resources in respect of compliance with GDPR. This includes the issue and contractual and procedural documentation, as described above, as well as the implementation of training for all members of staff.

SYS3 Limited provides step by step guidelines for all service support tasks and activities

Training is provided by SYS3 Limited management in-house to enable all employees and contractors to operate consistently.

3.3. Risk Assessment

SYS3 Limited has run an assessment to determine that our physical office environment, our IT systems, our personnel, our policies and our practices conform to the standards of the General Data Protection Regulation. This assessment has been extended to verify the GDPR conformity of our key suppliers too.

Our assessment includes a register of data, classifying the data that we hold, identifying where it is stored, and articulating where risks lie and how we can mitigate these The establishment of this register allows SYS3 to respond rapidly, if required, to data access requests.

We operate a formal incident management process to identify, contain, and recover from a data breach, should one occur. Our employees are trained to report any suspicion of data breach to our Data Protection Officer in line with our Data Protection Policy.

4. Suppliers & Third Parties

Qualifying the compliance of key suppliers and third parties is essential to establishing our own Statement of Compliance with GDPR. Should any suppliers or third parties with whom we share personal information – either as data controllers of data processors – fail to evidence conformity to the requirements of GDPR (or fail to ameliorate their non-conformity under notice) we will terminate our relationship with them.

Our current key suppliers/third party in the context of personal information data processing are as below, and have documented evidence of their compliance with GDPR.

Supplier	Privacy Measures & Statements
Iomart	https://www.iomart.com/privacy-policy/
Brigantia	https://www.brigantia.com/gdpr-compliance-policy-statement/ https://www.brigantia.com/wp-content/uploads/2018/05/Brigantia_Privacy_Policy_v1.0.pdf
Solarwinds	https://www.brigantia.com/wp-content/uploads/2018/05/Brigantia_Privacy_Policy_v1.0.pdf https://www.solarwinds.com/legal/privacy#privacy
Entanet	https://www.enta.net/legal/
Microsoft	https://privacy.microsoft.com/en-gb/privacystatement
Gigasoft	https://gigasoftdatabackup.com/pdf/GDPR%20Compliance%20Statement.pdf https://gigasoftdatabackup.com/pdf/Privacy%20policy.pdf
GoCardless	https://gocardless.com/legal/privacy
KCOM	https://business.kcom.com/privacy-policy/
VIA	https://via.co.uk/gdpr-compliance/

5. Physical Security

SYS3 Limited commits to protecting data through appropriate physical measures, these can be broken down into:

5.1. Premises Access Control

Access to all our office environments is physically controlled during business hours of 08:30AM to 05:00PM. Our premises are alarmed and a list of keyholders held at all times.

5.2. Server Access Control (Physical)

Servers, routers and other business critical equipment is stored securely.

5.3. Server Access Control (Digital)

Hosted (Cloud) Server access is via secure (SSL) connection. Passwords to confirm our password policy. Access to data is further restricted by IP Address.

All other systems where personal data is held are accessed either by MFA or secure passwords protected by a digital password vault. Remote access to servers is carefully managed and monitored with enhanced security protocols in place.

5.4. Portable Media

All portable media use by SYS3 Limited is subject to encryption and/or password control.

6. Cyber Security

SYS3 Limited has committed to ensuring that cyber security remains at the forefront of our day to day business. Along with advanced security and protection software in-house, our range of data protection methods include Data Loss Prevention and the use of Secure File Transfer Protocols.