Locstatt Data Security, Privacy & GDPR

Document Information			
Area Identifier:	Locstatt	USA : UK : AUSTRALIA	
Category Identifier:	MS	Locstatt Management System	
System Identifier:		Administration	
Sequence Number:			
Applicable Countries:	**USA**	**UK**	**AUSTRALIA**

Document Owner	Director & Senior Consultant Locstatt

Control Information:	
Security Standard:	Company Confidential
Control Number:	
Control Status:	Controlled

Document Review Category	C1	C1: 12 Months	C3: 36 Months

Document Revisions					
Rev	**Date**	**Description**	**Author**	**Reviewed By**	**Approved By**
1	30 October 2018	Initial Issue	B. Donaldson	J. Guillen	R. Donaldson
2	1 September 2020	Update Issue	J. Guillen	R. Donaldson	B. Donaldson

Contents

1.0 Locstatt's Commitment to Privacy and Data Security

The Locstatt privacy policy outlines our business practices in relation to the collection, storage and use of personal data gathered to facilitate client records within Locstatt. It sets out the purpose of data collection, the types of information collected and the scope and limitation of data processing within Locstatt.

1.1 Privacy Overview Comments

When reading this document the following should be noted:

1. Locstatt has agreements with our clients that details all data privacy policy and information.

2. Locstatt clients have employment agreements with their own company employees that covers required 3rd party information data transfer.

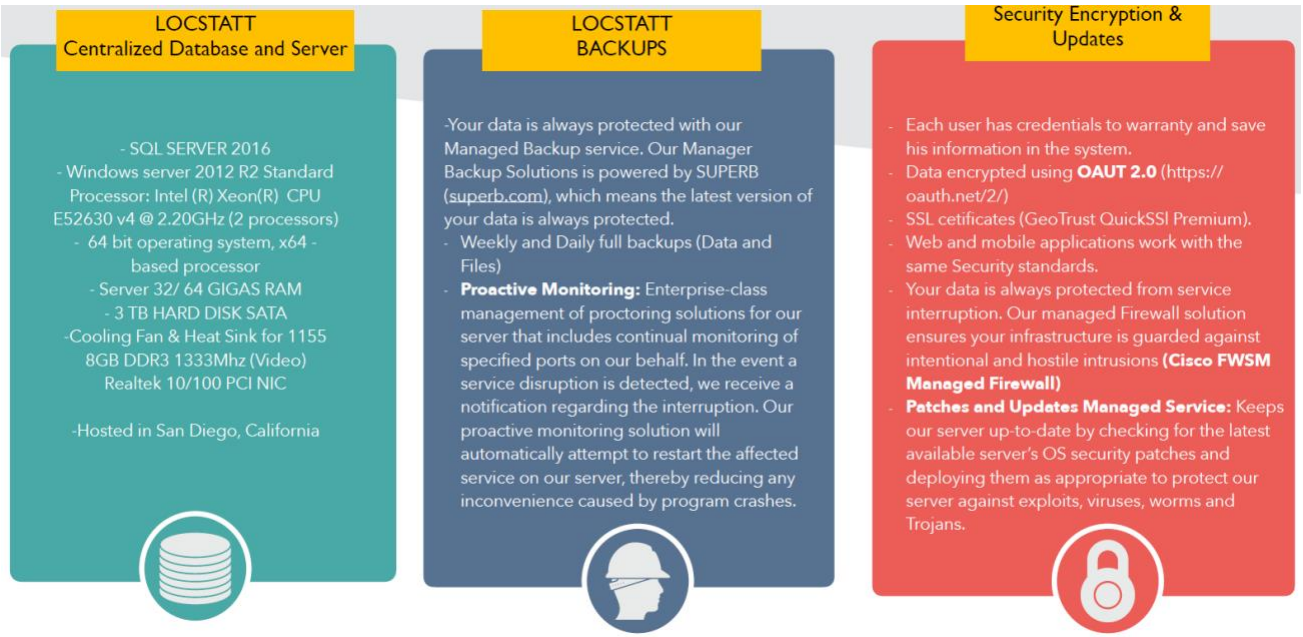
3. Locstatt will respond to client privacy data requests as related to their individual employees but Locstatt will not have privacy agreements with client company individual users.

4. The data centers used by our cloud providers are also subject to security compliance requirements around data jurisdiction. In the UK, the European Union's GDPR regulation has introduced new compliance requirements for customer data and Locstatt has systems in place to meet compliance.

5. Restriction of the type of personal information collected. When we first designed Locstatt we made provision to be able to collect a wide range of personal information. This included names, date of birth, home address, contact phone number, company, job position, driver's license number, home address, email etc.

   However we have now restricted the amount of personal information that we typically collect down to only name, date of birth, company and email address. Email address is only captured when creating Locstatt users which is only approximately 5 percent (supervisors & management) of all company employees that interact with Locstatt.

1.2 Server Data Security Overview



2.0 Privacy Policy Details

Locstatt LLC offer a suite of Health & Safety Apps, and we are firmly committed to preserving our client privacy. This privacy statement ("Statement") explains our online information practices and the choices you can make about the way your information is collected stored and used when you:

1. Interact or use our websites, including downloading materials from our systems, mobile or localized versions and related domains and subdomains (collectively the "Websites").

2. Register and/or attend any of our events, Help & Support meetings (collectively "Events").

3. Use any of our products, services or applications including any trial (collectively the "Services") in any manner. The "Services" means Locstatt's Health and Safety Software products, applications and services, in each case in whatever format they may be offered now or in the future.

4. Are issued a Locstatt identity number as a company employee or become a "User" of Locstatt Services (by definition, a User is a company employee with a Locstatt identity number & registered email).

2.1 Membership Package

Your use of these Services is governed by your organization's policies. We will only use, disclose and otherwise process Personal Information for the purposes set forth in your agreement with us for the provisioning of the Services as laid out in your organizations Membership Package and subsequent additions to your organizations Membership Package as agreed via email. Specifically the Membership Package, Section 2 states:

> *2.4 Personal data will be collected, processed and used by Locstatt for the purpose of providing the Service and to facilitate transactions that Customer enter into with Locstatt through the Service. Personal data will not be used for marketing purposes and will not be disclosed to any third parties (including advertisers and suppliers). All Customer information will be treated as confidential and shall not be disclosed to any third-party without the express written consent of Customer.*
>
> *2.5 Customer is responsible for the content and accuracy of data connected with the Service. Locstatt does not monitor or verify Customer input and Customer is wholly responsible for any inaccuracy or unsuitability of content added to the Service.*

As a company employee or User please direct your privacy questions or concerns to your employer or your organization's Locstatt Services administrators.

We respect the privacy rights of our users and recognize the importance of protecting the Personal Information we collect about you. We share your Personal Information within Locstatt Software and with third parties only as defined below. We may also share your Personal Information with law enforcement agencies or other bodies if we are required to do so by law.

This Statement does not apply to any website, product or service of any third-party company even if their website links to or from our Website. We are not responsible for the privacy policies or the content of these other websites as we do not operate or control these websites, products or services. You should check the privacy statement of other websites to determine whether you wish to share your Personal Information with them.

3.0 What information does Locstatt collect and why?

We gather various types of information, including information that identifies or may identify you as an individual; personally identifying information and/or personal data (collectively referred to as “Personal Information”) from Websites or Events, and from our Services.

For Example we may collect any Personal Information that you choose to send to us or provide to us on our “Request a Demo” (or similar) online form or if you register for any Locstatt Events. If you contact us through the Websites, we will keep a record of our correspondence. We may collect information when you interact with our postings and other content on third-party sites or platforms, such as social networking sites. This may include information such as “Likes”, profile information gathered from social networking sites or the fact that you viewed or interacted with our content.

We also receive and store information you provide directly to us from our Services, for example, when setting up new Users we collect Personal Information, such as name and e-mail address, to provide them with Services. The types of information we may collect directly from our customers and their Users include: name, job title, phone number, username, email address, transactional information (including Services purchased), as well as any other contact or other information they choose to provide us or upload to our systems in connection with the Services.

Any reference to Personal Information refers to any information that can be used to identify a specific person, or any anonymous information (such as an IP address) that is linked to a specific person. Personal Information does not include information that has been aggregated or made anonymous such that it can no longer be reasonably associated with a specific person.

We collect this information to help identify you and your session, to improve our website to ensure the content is presented in the most efficient manner, to gather broad demographic information, including troubleshooting, data analysis, statistical and survey purposes, this helps us to provide, maintain and improve the Websites and Services. Also for purposes made clear to you at the time you submit your information, for example to provide you with access to one of our Help & Support meetings, to fulfil your request for a Demo, and to provide you with information you may have requested about our Services. Ultimately the information gathered allows Locstatt to deliver the best customer service and product.

3.1 How does Locstatt use and protect your Personal information?

Locstatt does not sell or rent your Personal Information to third parties or marketers. We only disclose Personal Information to those of our employees, contractors and trusted affiliated organizations that are suitably authorized and integral to the operation of our Websites and Services and need to know that information in order to process it on behalf of Locstatt, or to provide services available at Locstatt websites.

We will disclose your Personal Information to third parties outside Locstatt in the following circumstances:

Third Party Service Providers

1. To send you post or email via third party communications or delivery service providers
2. To provide our customer service infrastructure including our help and support services
3. To manage how we follow up with enquiries
4. To update records that your company is using from third party providers, for example: Training records.

.

For a full list of the sub processors we use, See Appendix A

We may also disclose Personal Information in response to a court order, subpoena or other governmental request, or when Locstatt believes in good faith that disclosure is reasonably necessary to protect the property or rights of Locstatt, to report suspected illegal activity, or to investigate violations of our terms and

conditions. If we ask you to provide Personal Information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you accordingly.

If your organization is situated, and using our Services, within the European Economic Area (the“EEA”) then we will store and process your Personal Information on servers located within the EEA. Where we engage with third party service providers for operational reasons, we may transfer your Personal Information outside the EEA for example when a client company has an international presence in countries both within and outside of the EEA. We only transfer your Personal Information outside the EEA where the European Commission has decided that the country in question ensures an adequate level of protection in line with EEA data protection standards or there are appropriate safeguards in place to protect your Personal Information. The European Union (EU) law allows personal data to flow outside the EU only if there is an adequate level of protection in the country of destination or if a number of specific exceptions apply. If your organization is situated, and using our Services outside the European Economic Area, then in some circumstances we may store your Personal Information on servers located outside your country of residence. In all of these instances we will still take all measures reasonably necessary to protect your Personal information in accordance with this Privacy Notice against unauthorized access, use, alteration or destruction.

If you are an individual from the European Economic Area (EEA), our legal basis for collecting and using the Personal Information will depend on the information concerned and the specific context in which we collect it. In some cases, we may also have a legal obligation to collect Personal Information from you, or may otherwise need the information to protect your vital interests or those of another person.

We will normally only collect Personal Information from you where we have your consent to do so, or where we need it to perform a contract with you (e.g. to deliver the Services that you have requested).

Where we rely on your consent to process the Personal Information, you have the right to withdraw or decline your consent at any time. Please note that this does not affect the lawfulness of the processing based on consent before its withdrawal.

We will keep your Personal Information for no longer than is necessary for the purposes for which the data was provided. However when a Company or organization ceases to use our services, or a Query has been closed, (this includes Device information with an associated account) we may hold your Personal Information for a longer period, for example, if we are processing an ongoing claim or believe in good faith that the law or a relevant regulator may reasonably in our view expect or require us to preserve your Personal Information for a longer period, or to maintain system backups.

If you are a registered User of the Locstatt Websites and have supplied your email address, then Locstatt may occasionally send you an email to tell you about new features, solicit your feedback, or just keep you up to date with what's going on with Locstatt and our products. For information on how to Opt-Out of such communication please see our Choices & Opt-Out section below.

3.2 Cookies

Our site uses cookies to keep track of your visits and requests and to save your registration information so you don’t have to re-enter it each time you visit our site. The following information is stored in cookies and our webserver logs any visits to our Website:

1. Your IP address
2. The type of Internet browser and the operating system of the computer you use to access the site
3. The date and time you visit the site
4. The pages you visit on the site
5. If you linked to our site from another website, and the address of that website
6. If you linked to the site from a search engine, the address of that search engine and the search term you used.

To read our full Cookie Notice, See Appendix B

3.3 Choices and Opt-Out

You can choose to opt-out of email communications by contacting operations@locstatt.com You can also choose to not provide Personal Information or allow cookies to be placed on your computer however this will limit your ability to use our Services and disable many features available through our Websites.

If you would like to review, access, delete, update, or rectify any Personal Information we hold about you, or exercise any other data subject right available to you under the EU General Data Protection Regulation (GDPR) you can contact our privacy team on operations@locstatt.com

If you are not satisfied with the way we handle a complaint you make in relation to your Personal Information, you may be able to refer your complaint to the relevant data protection authority. In the UK this is the Information Commissioners Office (ICO). The ICO's contact details can be found on their website https://ico.org.uk/

4.0 Handling of Client Data on Client Request or Termination of Contract

(a) All Client Data will be treated as Company's Confidential Information. Where disclosure is required by applicable law, Locstatt will comply with all requirements as stipulated in the Contract for disclosure.

(b) Locstatt will only store Client Data on secure servers as detailed in Section 1.2 above. Except as agreed otherwise, Client Data may not be accessed by or transferred to Client Personnel or Users, outside the specified region for any reason, including Client support, operations, and troubleshooting.

(c) Locstatt will logically and physically segregate that Client Data from any other data held or managed by Locstatt, including data related to the Locstatt's other customers.

(d) Under the contract Locstatt receives no rights in Client Data except as necessary to provide the system online services.

(e) Locstatt will provide Client or its nominee all necessary access to Client Data that is not accessible through the normal features set of the Locstatt online services and reasonably required to enable electronic discovery, such as in legal disputes with third parties. If any of those requests results in an undue burden to Locstatt, the parties will negotiate in good faith regarding reasonable reimbursement of Locstatt's costs.

(f) Locstatt will maintain a notice and take-down procedure in respect of any third party claim asserting that Client Data through the normal features of the Locstatt online services infringe any third party right. If this was to occur, Locstatt would promptly notify Client of the claim and identify:

1. The relevant Client Data
2. Provide Client a reasonable opportunity to respond and manage the claim; and
3. Only remove Client Data from the online services, without deleting the information if there are reasonable grounds to suspect that Client Data infringes third party rights and Client has not responded to the notice of Locstatt within 30 days of receipt of Locstatt notice.

(g) At the end of the Subscription Period, Locstatt will permit Client, at Client's option, to retrieve or (except where such data is required by Applicable Law) delete Client Data.

If Client exercises that option, Locstatt will validate with Client whether the retrieval was successful.

After the retrieval, Locstatt will request formal permission to delete any and all remaining Client Data, and confirm the deletion (except where such data is required by Applicable Law). Client is entitled to have Locstatt audited to validate that the Client Data has been deleted.

4.2 Business Transfers

If Locstatt or substantially all of its assets, were acquired, or in the unlikely event that Locstatt goes out of business or enters bankruptcy, or goes through some other form of change of control, Personal Information could be one of the assets that may be shared, transferred or acquired by a third party.

How to Contact Us

Should you have other questions or concerns about these privacy policies, please send us an email at operations@locstatt.com

4.3 Amendments

From time to time this Statement will be amended and the Website will be updated with the most recent version. It is your responsibility to regularly review this Statement to ensure that you are familiar with the most current version. Your continued use of this site after any change in this Privacy Policy will constitute your acceptance of such change.

5.0 Technical Support & Development

This section sets out the Information Technology (IT) Policy for Locstatt for the protection of its IM&T systems and defining baseline responsibilities for IM&T security, equipment and file storage. “IM&T systems” refers to the Locstatt IT network, hardware including portable media, system and application software, communication components including WAN systems, documentation, physical environment and other information assets. It does not include IT systems not connected to the Locstatt IT network.

5.1 Information Technology Policy

This Policy covers the IT networks for Locstatt staff across all sites.

The equipment covered by this policy includes:

- Network Infrastructure – The equipment housed internally to provide the Locstatt IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices, NTEs, ATAs and remote access systems.
- Desktops – Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties
- Laptops - Portable Personal Computers issued or provided to staff in the course of carrying out their duties
- Mobile Phones/Devices - Digital communication devices issued or provided to staff in the course of carrying out their duties.
- Media/Portable Media – Electronic Storage Devices such as memory sticks and hard drives issued or provided to staff in the course of carrying out their duties.
- External Communications Infrastructure – Equipment used to connect Locstatt to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.

The objective of this policy is to ensure:

- The confidentiality of data and information assets are protected against unauthorized disclosure and incidents are promptly reported.

- The integrity of data and information assets so that they are protected from unauthorized or accidental modification.
- The availability and accessibility of IT systems as and when required by staff

This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented at Locstatt to ensure there is a centralized and consistent approach to IT security.

One of the aims of the policy aims to raise awareness of the importance of IT security in the day to day business of Locstatt.

5.2 Responsibilities

Defining responsibilities ensures that all users of Locstatt IT systems are aware of their responsibilities to minimize the risks to IT security and operations.

The Locstatt Business Manager is responsible for ensuring that:

- No unauthorized staff are allowed to access any Locstatt IT systems in any location, as such access could compromise data integrity.
- Named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege.
- Robust disaster recovery and business continuity procedures are in place.
- All current and new users are instructed in their security responsibilities;

The Locstatt Development Department has the following responsibilities:

- Day to day responsibility for the management and security of the systems, equipment and services including those outsourced to service providers.
- To make all users aware of this policy and to ensure that users understand and are able to abide by them when carrying out work for Locstatt.
- Monitoring and reporting on the state of IT security within Locstatt and across all Locstatt systems.
- Developing and enforcing detailed procedures to maintain security access to all Locstatt systems.
- Ensuring compliance with relevant legislation, policies and good practice for all internal systems.
- Monitoring for actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.
- Maintaining an IT asset register.
- The allocation/disposal/reallocation of all computer hardware and software to ensure best practice usage, value for money and that all data storage devices, including portable electronic media, are purged of sensitive data (such as confidential or personal information) before disposal or reallocation.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Purchasing all computer equipment and software/license to ensure value for money, consistency and compliance.

The Locstatt Administration group is responsible for ensuring that:

- All Locstatt staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and interns sign Locstatt standard confidentiality undertaking before they are permitted to use Locstatt systems.
- New staff are given basic user training in IT Security as part of their induction.

Users are responsible for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where necessary to disclose

them to the IT department for administrative purposes) and to deny unauthorized third party access to Locstatt systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the Locstatt IT department regardless of the working state of the equipment.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business in order to minimize the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.

5.3 Security

Technical security measures will be put in place to protect Locstatt systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

Email and internet use will be monitored.

Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

All relevant contracts with third parties will include standard clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the Locstatt Development group.

All IT equipment, including virtual systems, will be uniquely identified and recorded.

Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

Records of all faults and suspected faults will be maintained.

All Locstatt laptops must be encrypted with access to Locstatt IT networks via using a strong authentication method.

Memory sticks and other portable media must be encrypted or have password protection when sensitive data is being transported outside secure offices.

5.4 Software

Only licensed copies of commercial software or in house developed software are used by Locstatt. The Locstatt Development group will maintain a register of all commercial software, including all software licenses, to ensure that Locstatt complies with license conditions and relevant law. Users must not install ANY externally developed software on Locstatt IT equipment without prior approval of the Development group.

Users are reminded it is a criminal offence to make or use unauthorized copies of commercial software and that offenders may be liable to disciplinary action.

Software products required by any department should be approved by the Locstatt Development group. Unless otherwise directed all software purchasing and licensing will be carried out by Locstatt Administration.

Locstatt will minimize the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate national guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the Locstatt Development group as appropriate.

5.5 Physical Access Controls

The Locstatt main servers will be outsourced to hosting services where physical access is restricted and controlled by their process and procedures.

In the Locstatt offices, physical access controls to secure areas will minimize the threat to the Locstatt systems through damage or interference. The Locstatt Development group department will be responsible for access to all IT systems located in secure areas, with access being restricted.

Note: For clarification, the Locstatt Development office where the Developers work is a restricted area and access will be controlled by the General Manager and via use of the Locstatt Facility Logbook.

No remote access to Locstatt IT systems will be given to third parties at any time unless specific authorization is received from the General Manager. Such access if granted must be supervised at all times.

5.6 User Access Control to the IT Network

User access to the IT network drives will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves Locstatt. It will be the responsibility of the Administration group to notify the Locstatt IT department immediately of any changes required to access controls, and procedures will be established to ensure this happens.

No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

Users are not permitted to store entertainment files (including but not limited to music, pictures, video, electronic games) on the Locstatt systems. Files which have the same nature but are for work purposes must be approved by the General Manager.

5.7 Disposal / Reallocation of Equipment

Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated within a department (or any other user) and must always be returned to Locstatt IT for reallocation to ensure correct management of sensitive data

Where equipment is obsolete for Locstatt business purposes but is still in working order and is deemed to be of use to private individuals, that equipment will be offered for sale to Locstatt staff without any guarantees or warranties.

Where the equipment is deemed to be of no use to private individuals, it will be either disposed of in a secure and responsible manner.

5.8 Security Incident Investigation & Reporting

The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.

A security incident is an event that may result in:

- Degraded system integrity
- Loss of system availability
- Disclosure of confidential information
- Disruption of activity
- Financial loss
- Legal action
  Unauthorized access to applications
- Loss of data

The General Manager and Director will be immediately notified of all security incidents.

All users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.

All actual security incidents will be formally logged in the Locstatt Incident Reporting system.

5.9 Disaster Recovery & Business Continuity

All business critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

All data will be backed multiple sites so that data exist in four places. Critical computer equipment must be fitted with battery back-ups (UPS) to ensure that it does not fail during switchovers or emergency shutdowns.

To minimize the risk to Locstatt IT systems and Locstatt client data, robust disaster recovery plans will be put in place to ensure:

- Identification of critical computer systems
- Identification of areas of greatest vulnerability and prioritization of key users and user areas
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required
- Development, documentation and testing of disaster recovery plans with the Locstatt 3rd party hosted services, including identifying tasks, agreeing responsibilities and defining priorities

- The existence of emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel) and actions to be taken to return to full normal service

6.0 Locstatt Emergency Contact Details

USA Helpdesk Support	+1 (281) 886-0829
UK Helpdesk Support	+44 (0)7511 418264
Australia Helpdesk Support	+61 (0)4777 02342
Helpdesk Email	contact@locstatt.com
Contracts & Administration	+1 (832) 705-0833 operations@locstatt.com

Appendix A: Sub Processors

No.	Sub-Processor	Activity	Source
1	Cold Fusion	Email SMTP gateway and Chat lines & cookies module	https://coldfusion.adobe.com/
2	Google	Analytics	https://thedailymetrics.com/templates/analytics/
3	Let's Encrypt	TLS (HTTPS)	https://www.rapidssl.com/
4	OAuth 2.0	Protocol for authorization	https://oauth.net/2/

Appendix B: Cookies

No.	Cookie Name	Duration	Process
1	CFID	3 years	Cookie set by Adobe ColdFusion applications. Used in conjunction with CFTOKEN this cookie helps to uniquely identify a client device (browser) to enable the site to maintain user session variables.
2	CFTOKEN	3 years	Cookie set by Adobe ColdFusion applications. Used in conjunction with CFID this cookie helps to uniquely identify a client device (browser) to enable the site to maintain user session variables.
3	__Secure-3PSIDCC	1 year	It is used to deliver the most relevant and interesting advertisements for the user
4	SIDCC	1 year	This cookie carries out information about how the end user uses the website and any advertising that the end user may have seen before visiting the said website.
5	__Secure-3PAPISID	2 years	It is used to deliver the most relevant and interesting advertisements for the user
6	SAPISID	2 years	This DoubleClick cookie is generally set through the site by advertising partners, and used by them to build a profile of the website visitor's interests and show relevant ads on other sites. This cookie works by uniquely identifying your browser and device.
7	APISID		This DoubleClick cookie is generally set through the site by advertising partners, and used by them to build a profile of the

No.	Cookie Name	Duration	Process
			website visitor's interests and show relevant ads on other sites. This cookie works by uniquely identifying your browser and device.
8	HSID	2 years	This cookie is set by DoubleClick (which is owned by Google) to build a profile of the website visitor's interests and show relevant ads on other sites.
9	__Secure-3PSID	2 years	It is used to deliver the most relevant and interesting advertisements for the user
10	SSID	2 years	This cookie carries out information about how the end user uses the website and any advertising that the end user may have seen before visiting the said website.
11	NID	6 months	Used to store user preferences
12	ANID	6 months	Used for advertisements displayed on the web
13	1P_JAR	1 year	Cookie that transfers data to Google to make advertising more attractive
	SID	2 years	This is a very common cookie name but where it is found as a session cookie it is likely to be used as for session state management.