Data Compliance and Security V2.0

www.melded.io

We know data.

At Melded we know that working alongside Councils, Hubs or Music Services means sharing a responsibility to protect peoples' personal data. It's vital that we not only understand the threats that exist, but we continually strive to strengthen the measures we have in place to safeguard against them.

Having worked in the industry for 20 years, we've seen procurement processes for new suppliers become increasingly complex in response to the advancing threats. We're committed to delivering whatever is required of us to satisfy the regulations that govern our industry.

Hopefully this document helps you determine more easily whether Melded is a suitable supplier for you in terms of data compliance and security.

If there's anything you need further help with, please email **hello@melded.io** or call **0161 883 7111**.

Thank you,

Mike Ellis
Director

1.0 Regulations

1.1 Requirements

The UK government requires that councils ensure that suppliers of web applications follow a set of principles to ensure the confidentiality, integrity, and availability of council data. Where the data contains personal information, the supplier will be considered a data processor under the terms of the Data Protection Act 2018. - https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

1.2 Principles

The guidance we follow is known as the Cyber Security Principles, which is published by the National Cyber Security Centre. Guidance on these principles is published at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles.

We explain later in this document how Melded addresses each of the principles.

2.0 Location & Environment

2.1 Location

All Melded data is stored in the UK, specifically at Digital Ocean's shared Data Centre in **London**. - https://www.digitalocean.com/

2.2 Certification

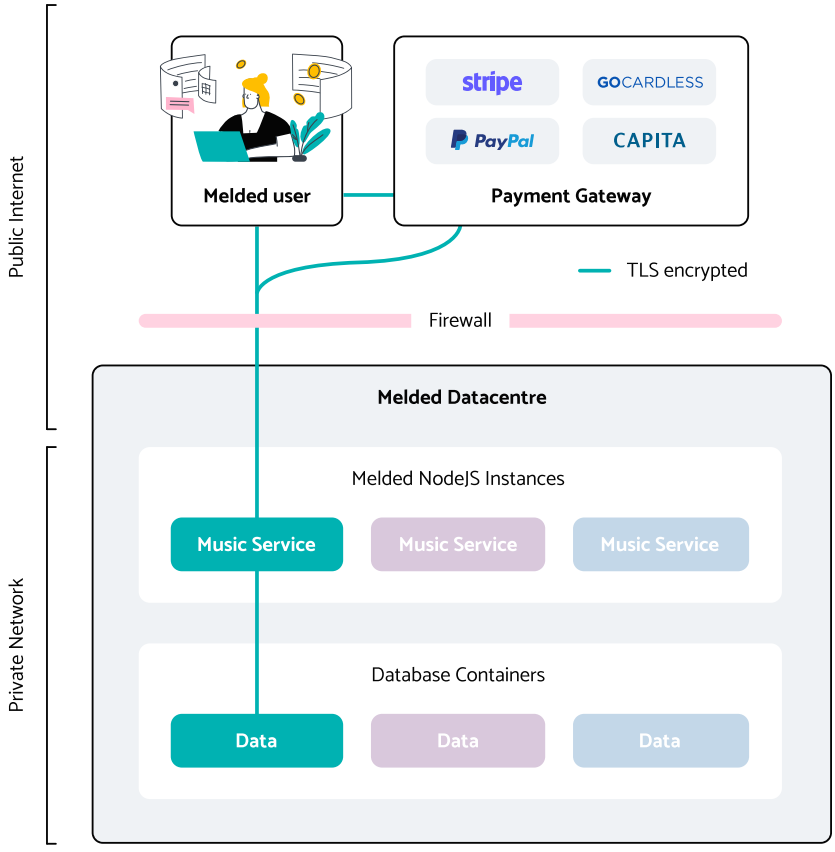
Our datacentre is **ISO/IEC 27001** and **PCI DSS** certified, and uses Next Gen Firewalls and IPS. Melded also employs application-specific protection ie. Web Application Firewall - https://www.gov.uk/data-protection

2.3 Technology

Melded uses a cloud computer model known as SaaS (Software as a Service) and is hosted off-premise at a Shared Data Centre. Technically it can be hosted anywhere. If you have specific requirements for hosting please email us at hello@melded.io or call 0161 883 7111.

2.4 Infrastructure

Melded has been designed and built from scratch with flexibility, scalability and security in mind. All data stored in Melded is transmitted via encrypted connections. Each Music Service has its own secure container in the database, accessible only by users belonging to that Service. Below is a High Level Design diagram that gives a basic insight into how Melded data is stored and accessed.



3.0 Identity & Access

3.1 Login

All users gain access using Username and Password, along with MFA (Multifactor Authentication) by either SMS (text message) or email verification where required. This includes our own Melded technical support staff, who are subject to secure access protocol.

3.2 Groups

Melded supports the use of groups for managing different levels of user access. Multiple user types are configured in the system and offer differing functionality. For example, a 'Staff' user is unable to perform an 'Admin' action, either directly or via API.

3.3 Logs

A log is kept of all user logins and any changes made to data. This can be reviewed for malicious activity and acted on accordingly.

3.4 Restrictions

Access to the Melded application can be voluntarily restricted by IP address, IP range and/or hostname if required.

3.5 Incident response

In the event of a breach or cyber attack, the relevant admin contacts will be notified in strict accordance with GDPR/DPA law. Any incident would be assessed for severity and dealt with promptly.

4.0 Operations & Security

4.1 Disaster recovery

As part of our Disaster Recovery procedure, weekly snapshot backups are taken automatically. Each backup is retained for four weeks, stored in the same datacentre as the server. Additional encrypted, offsite backups are taken of this data in the database.

4.2 Security protocols

Melded uses SSL, TLS (Organisation Validated). No non-standard web browsing ports are required. Our service is available on port 443 (SSL port). Certificate authority issued by R2.

4.3 Encryption

All data in transit (sent over network) is encrypted, and all stored data is 'encrypted at rest', whether on a disk or database.

4.4 Vulnerability management

Automatic security patches are applied to the underlying OS (currently Linux based) as and when they are released by the OS vendor. Application vulnerabilities are checked when the development code is pushed to the version control systems and resolved before being deployed to the live systems.

4.5 Updates

Updates are pushed as and when required to meet user needs. Before updates are published to the live system they are stress-tested internally. Updates are applied with a roll-back plan in place.

4.6 Data disposal

Whether requested by an administrator or dictated by GDPR/DPA, data is securely erased by overwriting methods when on shared hardware, or by hardware destruction if deemed necessary.

5.0 Backup & Recovery

5.1 Backups

Full disaster recovery backups are taken every week and are stored for four weeks within our shared data centre. Additional offsite backups of the database are taken at regular intervals, which are stored at another data centre managed by the same provider, under the same conditions as the primary DC.

5.2 Recovery

We aim for full recovery within 8 hours of determining the cause, nature and scale of any data loss.

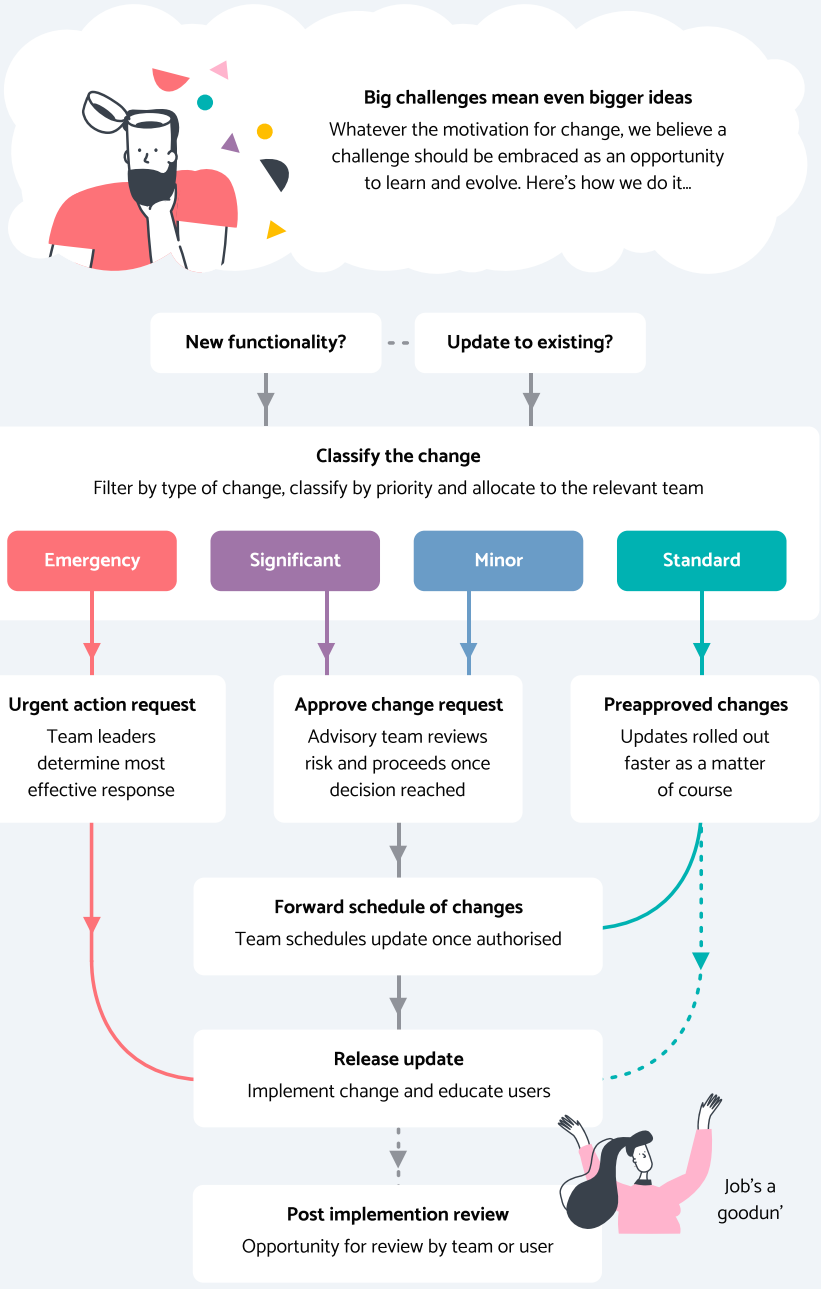
6.0 Methodology & Change Control

6.1 Methodology

The Melded team adopt a software development methodology known as 'Rapid Application Development'. We are a relatively small team and this allows us to react quickly to the needs of our users. We feel this methodology maximises our output and allows us the flexibility to develop solutions quickly, as well as being agile enough to benefit from advances in technology.

6.2 Change control

Below is an overview of Melded's change control process.



7.0 NCSC Cloud Security Principles

The National Cyber Security Centre offers these principles as guidance on how to configure, deploy and use cloud services securely. Below we explain how Melded addresses each principle.

1. Data in transit protection:

User data transiting networks should be adequately protected against tampering and eavesdropping.

All data being accessed and communicated within Melded is TLS v1.3 encrypted in transit. This is updated in line with the latest protocol versions.

2. Asset protection and resilience:

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

All user activity can be reviewed for malicious activity and acted on accordingly. All data is 'encrypted at rest', rendering it inaccessible should the physical drive be removed from the datacentre.

3. Separation between users:

A malicious or compromised user of the service should not be able to affect the service or data of another.

Clients can only access their own 'instance' of Melded, and their own database container. Accessing another client's 'instance' is not possible. A log of all user activity is kept on the server and any failed login attempts are recorded.

4. Governance framework:

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

Melded's data infrastructure is only ever as complex as it needs to be. It can adapt to the needs of the client, and to the changing requirements set by regulators. Only specified users have technical control eg Admins. Our goal is the unhindered cooperation between all users, while maintaining a secure and compliant environment in which to work.

5. Operational security:

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

All Melded processes are designed to be as efficient as possible. In the event that a threat is found it can be acted on immediately and the relevant administrators notified.

6. Personnel security:

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

Our team is small and made up of industry specialists. All personnel are subject to the same login restrictions applied to our client users. Login passwords set by client users remain hidden, even to our own developers.

7. Secure development:

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

Melded has been designed and built in-house from the ground up. Our team have an in-depth understanding of its processes. They are trained to identify any threats and act on them promptly.

8. Supply chain security:

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

Melded is modular, meaning it is fully scalable. This scalability ensures we offer a sustainable and robust system that can adapt quickly to any changes in security regulations.

9. Secure user management:

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

Melded features an advanced dashboard for Admins to manage their own user base. Different user types have configurable permission levels to grant/limit access to specific functions.

10. Identity and authentication:

All access to service interfaces should be constrained to authenticated and authorised individuals.

All Melded users require a registered email address and password, along with MFA (Multifactor Authentication). A log is kept of all user activity, as well as any failed login attempts.

7.0 NCSC Cloud Security Principles

11. External interface protection:

All external or less trusted interfaces of the service should be identified and appropriately defended.

Melded's codebase is entirely custom built, meaning it does not rely on any third party processes that could introduce a vulnerability. This allows us to retain full control over all security measures.

12. Secure service administration:

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

Melded Administrators do have higher permission levels and more control. However, they are subject to the same security protocols as any other user type. Should this privilege be abused, access to the Melded application can be voluntarily restricted by IP address, IP range and/or hostname. Data is continually protected against theft, by encryption in transit (sent) and at rest (stored).

13. Audit information for users:

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

User activity within Melded can be accessed and in the Reports module in the Admin dashboard, and exported to CSV. A more detailed audit of records over a specified time period can be made available on request.

14. Secure use of the service:

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

Melded has been designed to be easy-to-use, mitigating user error wherever possible and ensuring all new data being added to the system is as consistent and reliable as possible.