The Institute of
Clinical Science & Technology

Service Policy

Overview

99.5% website availablity

10 Hours of telephone support on weekdays (8am - 6pm)

24x7 Support for Severity 1 issues

Online access to documentation and technical resources, knowledge base, and disscussion forums.

Features

Hours of Operation:	10 Hours/Day Monday - Friday
Method of Access:	Telephone, Web, and e-mail
Number of support requests:	Unlimited
Business Hours:	Monday - Friday 8am - 6pm

Target Response Times:

Critical (Severity 1):	1 hour or less (24 x 7)
Major (Severity 2):	4 business hours
Minor (Severity 3):	8 business hours
Cosmetic (Severity 4):	12 business hours

Support Resources

www.clinicalscience.org.uk

The primary Clinical Science and Technology site provides an online support system through internal messaging, knowledge base, and support forum. In addition the site will contain resources to support all site users, such as instruction pages. Internal messaging and forum response times are consisent with published SLA based upon severity.

Telephone Support

Telephone support is available through normal office hours and 24 x 7 for Severity 1 issues, with response times consisent with published SLA based upon severity.

E-Mail

E-mail support is available through normal office hours and 24 x 7 for Severity 1 issues, with response times consisent with published SLA based upon severity.

The Institute of
Clinical Science & Technology

Severity Definitions and Response Targets

We provide a range of support times based on the urgency and severity of the support request. We do not guarantee resolution times - with no exceptions - due to the dependency on the nature of the reported problem and differences in the user operating enviroment (such as different browsers and devices).

Note: A full server restoration from backup takes approximately 1-3 hours to complete.

Severity Definitions

Severity 1

Definition:
Critical issue that severly impacts users use of the service, and no procedural workaround exists.

Examples:
Server failure
Inability of >20% of users able to access the site.

Severity 2

Definition:
Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact of portions of the user population and no reasonable workaround exists.

Examples:
Inability to use the website on >30% of devices or >50% of browsers

Severity 3

Definition:
There is a partial, non-critical loss of use of the service with a medium to low impact on the user population, but functionality continues. Short-term workaround is available but not scalable.

Examples:
Peer-to-Peer internal messaging not functioning.
Issue arises due to configuration changes by the user.

Severity 4

Definition:
Inquiry regarding a routine technical issue; information requested on website capabilities; navigation; or configuration issue; bug affecting a small number (<5) of users. Acceptable and scalable workaround availble.

Example:
Cosmetic Issues (Text alignment etc)
Errors in documentation
Issues impacting a single end user

Response Targets

In the event of a high priority issue, we strongly recommend logging your support request by phone to ensure the fastest possible response time.

Severity 1	1hr (24 x 7)
Severity 2	4hr (Business Hours)
Severity 3	8hr (Business Hours)
Severity 4	12hr (Business Hours)

The Institute of
Clinical Science & Technology

Website Availability and Maintenance

We work to meet a 99.5% of service availability. Availability is defined as the users ability to login to the system (website) and it performs to expectation. Service availability is measured on a month-to-month basis, and reviewed as necessary.

Downtime and maintenance

Unscheduled Maintenance
Unscheduled maintenance due to a Severity Level 1 or 2 may occur at anytime in order to restore expected website accessibility and functionality. This will be kept to a minimum, and all non-esstential works will be scheduled for completion under scheduled maintenance operations.

Scheduled Maintenance
Scheduled maintenance will occur during non-business hours and timetabled with periods of low website traffic to minimise disruption.

System Backup

A full database and files backup is completed each day. A database backup is done in addition every morning and evening. System restoration from backup takes approximately between 1 - 3 hours. This backup is automated at server level and is stored on a second proxy server. A second full backup is scheduled daily (currently 5am) and stored locally on the server.

Additional full backups are created manually immediately prior to any scheduled maintenance or system updates in order to minimise risks to data integrity and ensure a recent fully functioning version of the website is available to restore.

Data Centre Setup

UK Based

11KV diversely fed ring main supply

N+N UPS Infrastructure (A+B Feeds to Racks – 16A or 32A Commando's)

SDMO Diesel Generator with Auto change-over

N+1 Energy Efficient / Eco Cooling + Environmental Monitoring

24/7/365 HD CCTV Monitoring & Recording

10Gbps UK Network

Security Overview

This section outlines the procedures and methods of security on The Institute of Clinical Science and Technology's digital and online systems.

A secure server is vital for running any web software. ICST uses highly reputable partners to provide secure hosting and maintains impossible to guess password combinations for server administration. All correspondence and server administration is undertaken using encrypted protocols including file transfer.

Our Hosting providers maintain very high levels of security. All servers use:

a) Up to date PHP versions with the latest security fixes.
b) Apache in chroot-ed environment with suExec.
c) Sophisticated IDS / IPS systems which block malicious bots and attackers.
d) ModSecurity protection from the most common attacks.
e) A hardware firewall filtering flooding traffic.
f) A local software firewall based on iptables with more complex functions and traffic monitoring.
g) All services have a limit for the number of connections a remote host can establish.

Malware scanning can be included for sites with a high-risk profile to ensure systems are scanned continuously.

Keeping software up to date is essential for security and performance. Updates contain security patches for vulnerabilities, as well as improvements to user experience and functionality.

For complex sites, we recommend deploying updates on a development site. If an update is deployed without conflict, it can be deployed on the live site. For smaller sites, we run live updates and keeping full offsite backups in case there are issues. (See System Backup section above).

Some of the process ICST undertakes for core and advanced security of digital assets:

a) Daily backups.
b) Database prefix obfuscation.
c) Hiding admin login page.
d) Uptime monitoring.
e) Plugin vulnerability monitoring.
f) Security Audit Logging.
g) Disabling unused functions.
h) Trusted plugins and themes.

We only use, and recommend plugins and themes that have been well tested and reviewed by our team and the WordPress community. We don't install plugins that have low reviews or negative comments, as this could be a sign that the plugin developer does not follow good development or security measures. The plugins and themes we do use are very carefully curated and monitored for continuous performance.

SSL Security

HTTPS encrypts traffic sent to and from a server and makes it difficult for assailants to intercept data. For more active websites, and even for smaller sites, we recommend SSL certificates to help secure and protect onsite data.

When connecting to servers, we use SFTP encryption to encrypt passwords and other data as it is transmitted, so it cannot be intercepted.

User management

ICST ensures all team members are removed when they're no longer accessing the site, and Administrator access is only granted when needed. For example, users that will be adding content are only assigned appropriate access levels for their role, such as Author or Editor. We employ strict user management on all of our sites.

Any third parties or developers only have access to development sites, with updates tested and rolled out in a staged approach prior to going live.

Strong Passwords

No matter how good your security measures are, the most common way a website can be hacked is through use of insecure passwords. Through the use of automated scripts, hackers can attempt thousands of combinations

until they get in. For this reason, we use password generators for all accounts and keep this information stored in a secure cloud.

-The value of using a password generator is that they create complex, hard-to-guess passwords. ICST recommends a policy of enforcing the use of strong passwords and regularly updating them.

This is the most effective way to maintain a secure environment for a website, in summary:

a) Enforcing strong passwords.

b) Enforcing password updates periodically.

c) Multi factor authentication for high-risk sites.

Continuous Research and Improvement.

Security is not a simple thing, so our team at ICST undertake regular research to make sure we are providing the best solutions with an optimum mix of functionality and security. We take all security processes seriously with a pro-active approach, staying on top of the latest security protocols and research.

Criteria

Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the IT Manager or an appropriate manager who has been delegated this authority.

Risk Mitigation for discovered vulnerabilities

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

Assessment Levels

The following security assessment levels shall be established by The Institute of Clinical Science and Technology or other designated organization that will be performing the assessments.

The Institute of
Clinical Science & Technology

Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Gareth Davies
IT Manager
gareth.davies@clinicalscience.org.uk