Data Protection

How Does Criticall Safeguard My Data?

How Does Criticall Safeguard My Data?

Introduction

Any personal data given to Criticall by its Clients is for use within its hosted notification systems only, to deliver the services that it is contractually obligated to provide.

Client personal data (staff ID, home telephone number, etc) is only actively used by the system when a Call-Out has been initiated. A Call-out can only be initiated by approved users within the Client, or exceptionally by Criticall support staff on the express instructions of the Client.

Criticall takes seriously its duty of care regarding data, to guard against loss, theft, copying, corruption, or any form of misuse, or abuse.

The purpose of this document is to set out the steps that Criticall take to safeguard personal client data entrusted to it as a company.

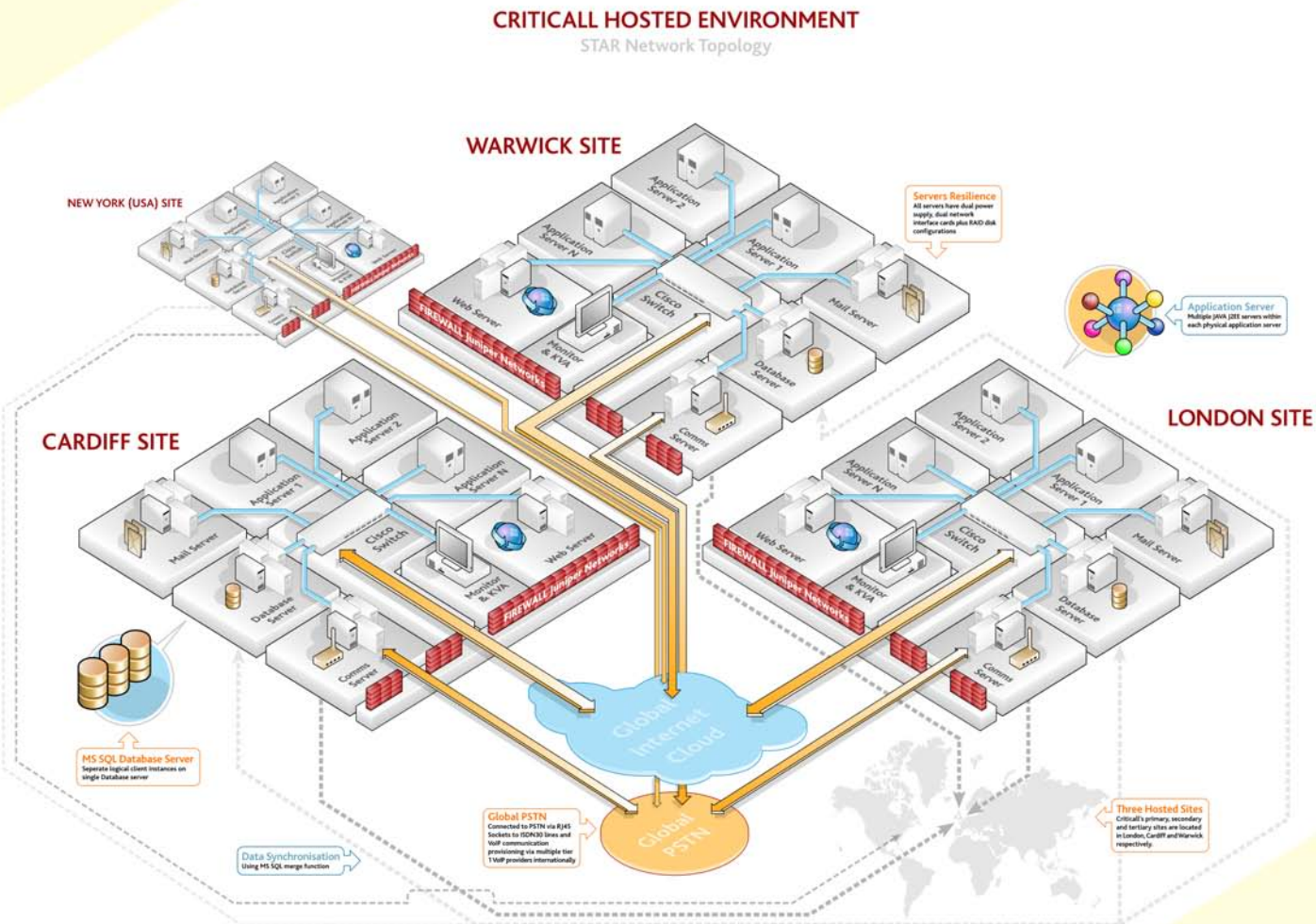
Information Security Governance Model

Within Criticall, responsibility for data is owned at the relevant level for each type of data. Client account data is owned by the Vice President of Business Development (VPBD), Marketing Data is owned by the Marketing Manager, Operational Data is owned by the Operations Manager (OM), corporate data is owned by the CEO, who is also the contact point to address any perceived, or potential breaches of Criticall's compliance to stated information security policies. Individuals are responsible for their own data relevant to their need to access and handle it, respective to their roles. Production system password access is given just to the extent required to perform support tasks. Not even the CEO, or Board have access to Client data. Sharing of data internally & externally is governed by the Data Protection Act, plus specific NDAs and other contractual arrangements with clients and suppliers. Sharing of client data is on a need to know basis, consistent with the relevant contractor or member of staff to perform their necessary role. Staff are trained and instructed to treat all client data in accordance with prevailing data protection legislation and industry good practice.

All personal data held within the EmergencyCall system is governed by the UK's Data Protection Act 1998 and Criticall is governed by the UK's Data Protection Authority (Registration Number Z9697952 with the Information Commissioner's Office, www.informationcommissioner.gov.uk).

It also actively complies with the USA/EU Seven Safe Harbor Principles (www.export.gov/safeharbor) and this document forms an essential part of that compliance. Any queries, issues, complaints, or other procedural matters relating to Criticall's compliance with these acts should be directed by email to support@criticall.co.uk and/or by contacting us by telephone on +44 (0)870 351 4910, where it will be escalated to Criticall's CEO for resolution.

Independent recourse in such matters is available through the UK's Data Protection Authority. This document is itself made available via the company's web site at www.criticall.co.uk. Over and above the protections provided by these acts, Criticall enforces the following security measures to further safeguard customer data.



STAR Network Topology

Criticall
global enterprise messaging

Physical Security

The services are provided from platforms installed at Criticall's contracted secure hosting sites in London, Cardiff and New York. Hosting sites are managed by specialist data centre operations companies and share the following security features:

- Access to server rooms is restricted with biometric scanning, personal swipe card and PIN protection.
- Access is by prior arrangement only
- Premises are controlled by 7x24 security staff on site
- All key areas, both inside and outside the building, are kept under CCTV surveillance 7x24
- Those accessing the server room must be accompanied to the location
- Criticall's servers are housed in a lockable cabinet, with only hosting centre staff having the key
- Delivery, reception, loading and server room areas are all segregated from each other and each has its own access permissions
- Access to the server rooms from floors above and below is controlled by the same data centre service provider
- Third parties, such as hardware maintenance engineers, can only access the specific Criticall cabinets by prior appointment & accompanied by Criticall, or designated data centre staff.
- Modern Fire suppression equipment and systems are used throughout each data centre
- Water & leak detection equipment operates to detect any damaging water actions which might harm the data centre equipment
- As a central strand of its Backup Policy, Criticall don't store Client staff contact data on any media outside of the data centre (such as off-site tape, CD, or printed off copies). Any data handed to Criticall on such media by Clients is physically destroyed after use
- No Client data regarding employee contact details is held at the administrative headquarters, at 3 Chiswick Park, 566 Chiswick High Road, London W4 5YA. Only commercial and account specific information is held at the HQ (eg contracts, NDAs, invoice copies, etc)
- HQ office building physical security is controlled by an electronic pass card system to the office. The door is never left open without a member of staff being present in the room at all times. The HQ building has 24 hour manned security, with CCTV. Electronic records are kept of all access to the office 7x24 via a building management system, including access by office landlord staff and agents (eg cleaners)
- All sensitive materials held in locked cabinets

Logical Security

- Client access to Criticall's hosted notification systems is via a secure Web interface. Criticall secures its web interface using Digital Certificates with SSL for all connections between customer web browsers and the hosted system. As such, all traffic is encrypted. Criticall rotate these certificates on a regular basis.
- Criticall's entire hosted infrastructure and associated services are tested regularly by a specialist external system security company, called SecureTest. SecureTest are one of only a few companies authorised to accredit systems to the UK Government's CHECK certificate level, approved by the CESG. SecureTest conduct a range of tests following a detailed method, covering brute force, penetration and vulnerability assessments. Their findings are shared with Criticall's CEO. Information regarding their approach and their findings is available for viewing by Clients upon request and by appointment.
- In addition, Criticall periodically undertake further specialist vulnerability assessments, including SQL injection vulnerability, script hacking and other potential privileged access abuses.
- Firewalls protecting the server environment have IDS (Intrusion Detection System) software installed preventing unauthorised access to the secure network. Criticall employ a specialist third party to deliver its firewall monitoring and management services. Each firewall is loaded with intrusion detection software kept up to date with an ongoing latest release software support contract.
- Each hosted site is protected by the combination of a firewall and a de-militarised zone (DMZ) to defend against various denial of service and automated web-based attacks
- Criticall's High Availability Option Clients have their services hosted on two separate sites, kept logically separate and accessed via different URLs.
- Access to the production servers is achieved by support staff via secure VPN connections, of which only 5 are approved across the company.
- Production systems are not connected to any other networks.
- Corporate server passwords meet the elevated password format standard.
- Criticall's hosted services are periodically reviewed by external auditing bodies, including Client own outside service provider (OSP) audits. Details of these can be made available to Clients upon request.
- Criticall follow procedures and practices to BS7799 security standard and BS25999 Business Continuity standard levels

Data Security

Data held within Criticall hosted systems for each client is held on a unique client database. As such one Client's data is completely separated from other Clients. There is no risk of unauthorised transfer between databases.

Criticall's standard procedure is that any data sent to Criticall from Clients is encrypted using SSH to transfer data electronically to a secure location. Exceptionally, when physical media must be used, Criticall recommends PGP (or other suitable encryption protocol requested by the Client) while in transit. In most cases, the Client holds the Master database and Criticall only periodically receives the encrypted files of inserts, deletes and changes, as part of an automated process.

Criticall separates out Development and Test environments from its production Primary , Secondary and Tertiary systems. No Client data is used on Development systems. Data on test systems will be that provided by the Client themselves. Test environments are subject to the same physical and logical security measures employed on Production systems.

Staff Checks

All current staff have been with company for minimum of 5 years and have no disciplinary incidents in their history. Background checks are conducted on all new employees.

Other Criticall Security Procedures & Practices Around Data

1. Access to systems by staff is confined to identified users thereby ensuring accountability.

2. When accessing the system, all staff prove their identity by means of a unique authenticator which is secret, available only to the individual and never printed (except for relaying to the holder) or displayed, ie. password, personal identification number (PIN) or secret code. Criticall staff also use a unique identifier (a UserID) to distinguish themselves to the computer system.

3. Each person granted access is responsible for ensuring that their unique authenticator is not compromised, and the unique authenticator is changed if they believe this has occurred, advising their security administrator of the circumstances.

4. Staff are able to set up passwords known only to themselves, and are able to alter those passwords when they wish. Passwords have a minimum length of 6 characters and are designed to not be easily guessed.

5. Internal password systems periodically force holders to change their passwords and password systems ensure that when users change their password, they cannot revert to using their old password for at least 5 consecutive password changes.

6. Any passwords entered incorrectly three times in succession are revoked temporarily.

7. Where company laptops in use by staff have the capability of recording a number

of keystrokes, including User Id and password entry, and then replaying them on the screen, this facility is disabled.

8. Access to systems is within pre-defined hours. Exceptional access to systems outside of these pre-defined hours has to be specially authorised by the OM.

9. Persons do not hold internal system passwords which would allow them to carry out alone operations which require dual control or would grant them a level of authority to which they are not entitled.

10. Access control systems have the facility to enforce segregation of duties

11. Where there has been no user activity for a predetermined period of time, internal systems lock the user out and request re-authentication of the user before further activity.

12. Systems detect and deny access by unauthorised personnel or systems, as well as detect misuse of computer facilities, record such attempts, automatically disable such accounts and report them promptly for thorough investigation.

13. Audit trails of unauthorised access attempts are retained for review for a year by Criticall Management, together with the results of any investigations undertaken.

14. The Security Administrator (OM), or his deputy, ensures that all requests for the provision of access to computer systems are appropriately authorised by the CEO.

15. Systems have the facility to provide the Security Administrator with sufficient information to enable the administrator, or his deputy, to control and review authorised users and their permitted functions.

16. Audit trails are kept detailing System Administration activities.

17. Where client data is passed on telecommunications links which extend beyond the physical control of their premises, it is protected by encryption.

18. Local Development & Support personnel do not have access to live client confidential data and software, current or historical.

19. Client data is segregated away from other data and any other third party's data whilst on the Local Servers.

20. Where access to privileged functions, or client data has been granted temporarily to support personnel to provide emergency support, such access is withdrawn immediately following completion of the support task.

21. Local operators are restricted to those tasks, facilities and utilities, that their normal daily duties require except in exceptional circumstances, e.g. system or software failure. In such circumstances, any variation is logged, usually automatically, and reviewed by management.

22. Utilities and privileged access which provide the means to make uncontrolled changes to data on the system are not available to system operators.

23. Anti virus tools are installed on all servers and clients and are kept regularly updated

24. Criticall use industry recognised System Development Life Cycle models for all new development work, using a combination of the Waterfall and Iterative models, depending on circumstances.

25. Penetration testing is carried out on the infrastructure and systems by SecureTest, a specialist outside contractor, authorised to certify to the CESG's CHECK certificate and above.

26. Updates to the web site are controlled using strong authentication mechanisms e.g. hardware authentication. All changes automatically logged and tracked from initial request to implementation using an auditable change management system.

27. The platform is monitored for unauthorised changes on a regular/continuous basis using appropriate software tools

28. There is a formal process in place for responding to/dealing with Security Incidents, which directly involves the OM & the CEO

29. Cryptographic key information, unless encrypted or held in a tamper resistant environment, is kept in secure conditions under dual control of persons with split knowledge unconnected with the sending and receiving of messages.

30. No passwords are transmitted or stored in clear at any time.

31. ESCROW – Criticall provide Clients with commercial security and peace of mind, by placing its entire platform software suite in escrow. This is maintained on an individual client basis, under Agreement 38072 with NCC, at Manchester Technology Centre, Oxford Road, Manchester M1 7EF.

Client Data Protection

Criticall do NOT keep paper copies of client data. All data is stored on secure servers in secure data centres and all backups of client data are stored on encrypted drives.

Criticall stands by its commitment to protect personally identifiable client information - including names, telephone numbers, pin numbers, passwords and any other personal information provided to us - and to keep the privacy promises and contractual data commitments made. Information is secured in accordance with the 8 principles of the Data Protection Act 1998, namely:

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In accordance with the Act, each hard disk that is physically removed from one of our servers (including broken hard drives which are retained under our maintenance contracts) is wiped clean of all data and software in a 4 step process:

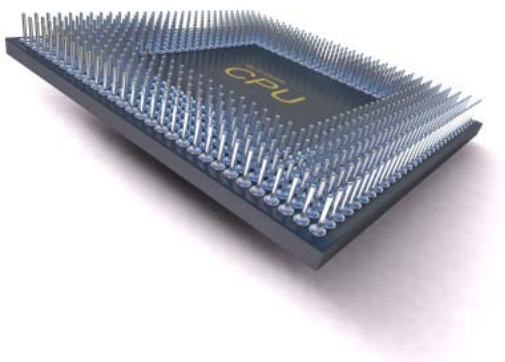
1) The Guttmann method is first used to purge client data whereby data is overwritten 35 times with carefully selected patterns which makes it unrecoverable. This is far more secure than even the United States Department of Defence recommendation which only requires data to be overwritten 7 times.

2) The hard drive is then re-formatted.
3) We then use an onsite data disposal company to wipe the data on the drives to HMG Infosec Standard 5 [CESG], supervised by an approved, senior member of Criticall staff
4) Finally the drives are then shredded and a certificate showing their destruction is provided and retained.

The onsite disposal team use mobile degaussers, which render magnetic media completely unusable and in addition damages the storage system. This is due to the devices having an infinitely variable read/write head positioning mechanism which relies on special servo control data, that is meant to be permanently embedded into the magnetic media. This servo data is written onto the media a single time at the factory using special-purpose servo writing hardware.

The servo patterns are normally never overwritten by the device for any reason and are used to precisely position the read/write heads over data tracks on the media, to compensate for sudden jarring device movements or changes in orientation. Degaussing indiscriminately removes not only the stored data, but also removes the servo control data - and without the servo data, the device is no longer able to determine where data is to be read, or written on the magnetic medium.

If a client's contract ends (or we receive an earlier formal client data removal request), then on the agreed day, all of their user data, historical reporting and database backups are immediately wiped from the Servers at each of Criticall's physical data centres, using the Guttmann method as described above. Once the data has been removed, the Criticall account manager will notify the main contact at the registered client's organisation by telephone as well as in a concluding email confirmation message.



criticall limited

3 chiswick park, 566 chiswick high road,
london, W4 5YA

tel: 0870 351 4908

fax: 0870 351 4907

web: www.criticall.co.uk

email: info@criticall.co.uk

www.criticall.co.uk/tour

Criticall
global enterprise messaging