Security. We love I.T.

CLARITAS
SOLUTIONS
www.claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

Security...
Ssh. We have the key.

Why Claritas:

Founded in 1997, Claritas Solutions provides independent IT services and solutions across all industry sectors.

Claritas works closely with clients to understand business strategies, utilising an independent approach to defining solutions that underpins a clients business objectives.

Claritas design solutions to enable companies to gain a competitive advantage, whilst reducing costs and mitigating risk.

Claritas work with organisations in a variety of different sectors, ranging from manufacturing to finance in the private sector and securing some the UK's most prominent public sector organisations such as police and government departments. These organisations rely on the IT team of technical experts to deliver truly exceptional 24/7 service, and to ensure the smooth running of their own businesses.

Contents:

Why Claritas 1
Information Security 2
Compliance 3
Network Security 4
Content Security 5
End point Security 6
Summary 7

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

The Claritas clear thinking introduction to... Information Security.

Information Security is the methods and measures deployed to safeguard information and data assets from a series of threats.

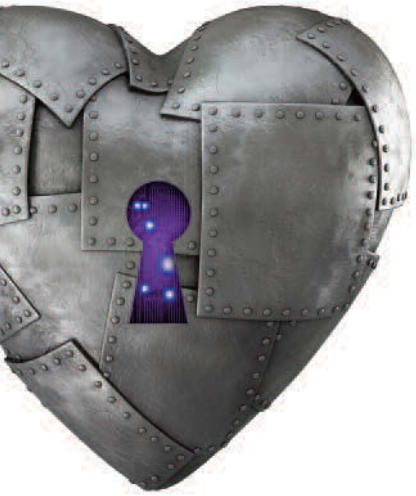
This can range from the physical security i.e. locks and alarm system, protecting access to individual computer equipment to encryption and biometric techniques preventing unauthorised access to information.

Information Security also covers the availability of data and the resilience of information systems particularly for failure or "disaster" scenarios.

Key to all information security is confidentiality, integrity and availability, these three principle's form the basis of the international information security standard, ISO27001. For the purposes of this document, we are concentrating on confidentiality and integrity, in our other papers we talk about the essence of availability, principally business continuity and disaster recovery, this is covered in the hosting document.

The Need for Information Security

Businesses are increasing reliant upon information. Whether that is information on clients, employees or suppliers, the need for more information is providing companies with the ability to gain competitive advantage over its competitors. What's more this need is only going to continue as businesses look for ways of making greater efficiencies.



Critical to organisations day-to-day operation is information flow, which covers customer information, client lists, stock and inventory information, supplier details, financial information, personal or payment information relating to individuals. Increasingly information is stored or "digitised" using computer and database systems, and it is critical to ensure all is protected from unauthorised access, tamper or deletion.

These can include competitive advantage, preventing loss of reputation, and compliance with legislative/industry/regulatory guidelines and requirements.

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

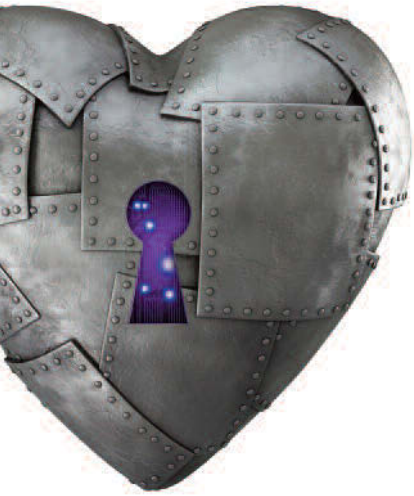
The Claritas clear thinking introduction to... Information Security.

Compliance

A substantial motivation for implementing information security processes and solutions is to ensure that an organisation is in accordance with relevant legislative and regulatory standards..

Over the last 10 years, many restrictions have been introduced to cover the electronic collection, storage and transmission of information. Recently the Information Commission Office [ICO] issued substantial fines for data breaches, where information concerning members of the public has occurred. These breaches range from loss or theft of laptops and memory sticks, to malicious hacking and public disclosure from so-called "hacktovists".

In addition as an attempt to combat credit card fraud on the Internet, members of the credit card industry (Visa, Master Card, American Express, etc.), have collectively devised a data security standard. This details how credit card information has to be processed and handled, particularly within electronic systems. This standard is the Payment Card Initiative Data Security Standard, [PCI/DSS] and must be adhered to before the credit card companies will allow business to be transacted using their systems. Failure to adhere to such standards can result in significant fines or ultimately could remove the ability for the businesses to transact credit card payments.



Physical Security

This involves securing physical access to an operating environment and computer hardware that is providing the information system. Secure premises need to have adequate doors, walls, locks, intruder alarms and manned security patrols. It is common to place computer equipment that "host" sensitive information in a data centre environment, where lots of systems can benefit from the deployed security measures.

Physical security covers how system components are protected, and how they are physically accessed i.e. access procedures to data centres, policies for removal or introduction of computer equipment from a secure location, etc.

Please see the "Introduction to….Hosting" guide for more information.

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

The Claritas clear thinking introduction to... Information Security.

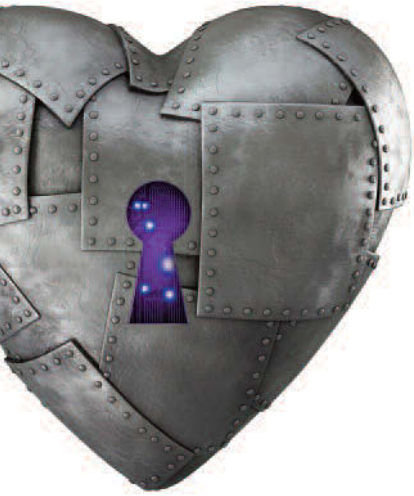
Perimeter/Network Security

Information systems and their associated data stores are increasingly becoming connected to computer networks, both public and private, so that they can be accessed by user-bases. This presents specific challenges to ensure a safe and secure environment. To guarantee a safe environment, strictures have to be engaged so only authorised users can access resources, that access is restricted to relevant system areas, that all access is monitored and any attempts to break into the system or disrupt access, are prevented.

These measures are introduced at network boundaries, where data enters and leaves the protected network space, and are generally referred to as Perimeter Security.

The most recognisable device that provides perimeter security is a Firewall. Firewalls control which data "packets" two computers can exchange, and what application and service can be used.

Firewalls have been used for many years as the first line of defence against network attacks and unauthorised access. Lately, "next generation" firewalls and Unified Threat Management (UTM) devices have become popular. These offer more protection. They tie in with authentication systems so users rather than computers can be given access privileges, in-built anti-virus and anti-malware protection, or advanced content security (see below).



Intrusion Detection Systems and Intrusion Prevention Systems (IPS/IDS) are now more accepted at the network perimeter. These kinds of solutions are designed to recognise and prevent abuse of the network/server infrastructure application or application code. Malicious attackers are able to launch many types of attack so it is crucial to any information system that these can be detected and blocked. IPS/IDS systems are updated regularly, much like anti-virus software, to ensure that they recognise new threats and hacking techniques.

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

The Claritas clear thinking introduction to... Information Security.

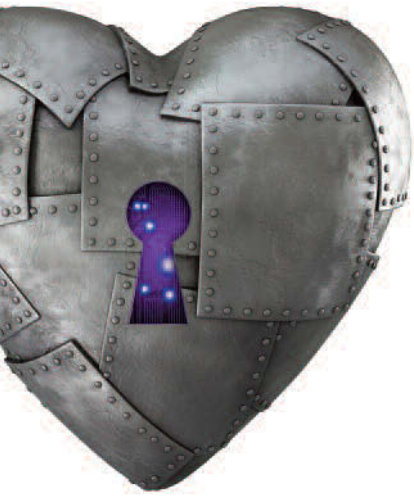
Content Security

Many organisations have a usage policy that defines exactly what users are allowed to and not allowed to access using the infrastructure. This can include anything that is illegal or inappropriate, such as pornography, hatred or racism, or content that could affect the productivity of the work-force such as gambling or shopping.

Content Security monitors and enforces what users can do with their computers and on the Internet.

The main areas are:

- Anti-virus/Anti-spyware/Anti-Malware protection - Performing scans and checks on email, web sites, web downloads and removable storage, such as USB sticks, portable hard-drives, mobile phones, etc, to ensure that no un-wanted or malicious programs are able to enter the organisation.
- Email Scanning – spam detection and management, which also may involve email confidentiality/encryption, archiving or business continuity.
- Web or URL filtering –the classification of websites and monitoring/controlling their use.
- Application Control – An extension to web filtering, which takes into account new web application/widgets and social media. For example a site like Facebook has thousands of applications built into it and numerous ways for users to interact. It may be desirable for some parts of the Facebook site to be accessible to users, but not to others. You may want the marketing team to be able post on your company's wall or respond to customer's queries using messaging or chat, but you don't want people to be able to play games. Application control is able to recognise different application or forms of communication "embedded" into web sites, and monitor and control their use.
- Data Loss Prevention (DLP) – Is the control and monitoring of information and how it leaves an organisation in a digital format. This can be as simple as detecting a sensitive or confidential email has been sent to the wrong recipient right up to preventing malicious exporting of company intellectual property.



DLP solutions usually have some way of classifying data within the organisation, such as database format, customer lists and corporate templates. They also have generic in-built data such as national insurance numbers, passport and driving license number from various countries, credit card numbers, pay roll or salary information. This allows the DLP system to recognise information when it is being sent outside the organisation and block as required.

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

SECURITY
We love I.T.

The Claritas clear thinking introduction to... Information Security.

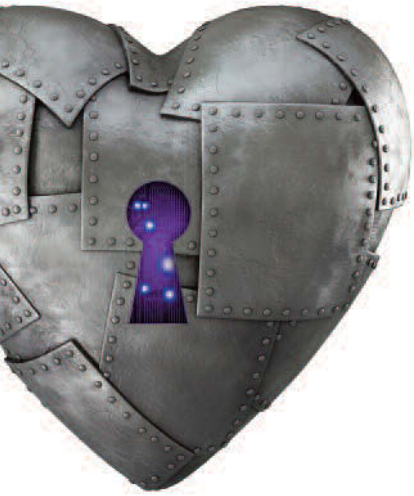
End-point Security

The locations where users interact with company systems have changed over the last few years, and remote or home working has become more wide spread, and the range of different device to interact with business system has increased. These devices include laptops, home computers, smart phones and tablet PCs, which are very often not owned or managed by the IT team.

End-point security is the way devices which are outside the traditional perimeter, and their related system communications, are managed in a safe and secure environment.

End-point Security allows:

- Secure, remote connections with the necessary authentication and encryption protection, using VPNs or external portal and extranets;
- Anti-virus and Anti-malware protection for remote devices.
- Enforcing corporate security policies (Web/URL filtering, application control, email security) on remote laptops
- Mobile Device Management (MDM) which includes data encryption, device tracking, and remote lock and wipe in case of theft or loss.
- Restricting and encrypting removable storage devices such as memory cards, USB sticks, etc.



Security Testing

As with any critical engineering discipline, testing and verification is an important part of the system lifecycle. Ensuring that the technologies and counter-measures that have been deployed are working correctly becomes an on-going process of testing and fixing.

Some testing methods, referred to Vulnerability Assessment or Penetration Testing, usually mimic real security incidents, and can be performed automatically or by trained personnel. Known exploits and "hacking" techniques are used against all aspects of the target system, with the intention to compromise or circumvent the installed security.

The testing exercise generates details of the methods used in the assessment, exploits or misconfigurations that have been found, and details of the remedial actions needed to "plug the gaps".

Usually security testing is executed by the specialists responsible for the installation or day to day management of the security solutions, which ensures no conflict of interest.

Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com

CLARITAS SOLUTIONS
Think Clearly, Think Claritas.

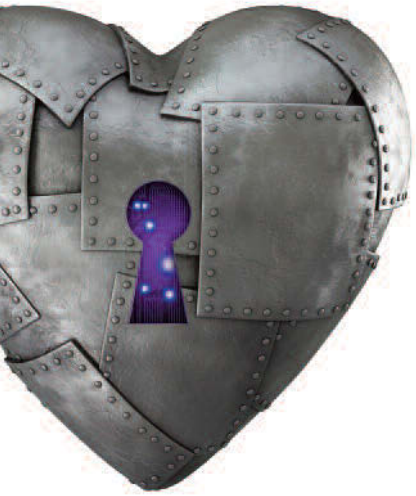
SECURITY
We love I.T.

The Claritas clear thinking introduction to... Information Security.

Summary

In short, information security is critical in an age where information is king. Whilst we have discussed different ways of safeguarding information, the reality is that information security is an ever changing landscape; there are constant advancements in technology to ensure that information is kept secure. The key to ensuring that your information is always secure is to engage a specialist that is constantly looking for solutions that mitigate the continual threat from information compromise.

and we want you to LOVE I.T. too



Claritas Solutions
West Wing, Bowcliffe Hall,
Bramham, Wetherby
LS23 6LP
T. 01937 849 966
E. contact@claritas-solutions.com