ONLINE<>50

In Safe Hands

Online50 & Information Security

The Online50 Service is run by IT Inside Out Ltd (ITIO); who have had the operation of the service accredited to the ISO 27001 standard for Information Security.

What is Information Security?

Information Security deals with the:

- Availability
- Integrity and
- Confidentiality

of Information.

The **Availability of Information** is whether or not it can be both accessed and operated on when required.

The **Integrity of Information** is whether or not the information is altered.

The **Confidentiality of Information** is whether the Information can be accessed by unauthorised users.

What is ISO 27001?

ISO 27001 is the International Standard for managing Information Security. To be accredited as reaching the standard organisations have to demonstrate that they have properly planned, documented and implemented appropriate measures for Information Security, as well as undertaken continuing reviews of their systems to ensure compliance and to identify improvements. The certification is only granted following an external audit by a recognised competent body.

As Online50 have been audited and accredited to the ISO 27001 standard you can be confident that we have properly implemented an Information Security regime to protect your Information.

The ISO 27001 standard does not dictate what policies and procedures should be adopted. To help you understand how we protect your information this document provides an overview of part of our Information Security management system.

How we protect your Information

We offer a higher level of Information Security than any other Online Accounting provider in the UK because the **scope of our operation is broader:**

IITO own and operate all of the infrastructure that the Online50 service operates on. Our Information Security management system covers all of the systems we operate. As we are an Internet Service Provider this means that we include the operation of everything required to provide the service, not just the operation of an application server. If you use an Internet access product from ITIO, then we are responsible for your information from the point it leaves your premises, for processing and storing of your information within our network and for the return of it to you.

Clearly we are not responsible for systems that we do not operate. This includes your own equipment, other systems that are part of the Internet, any information transmission that is outside our network and the actions of people not appointed by us.

Some of the considerations of our Information Security management system are:

Policies which govern our objectives and stipulate relevant contractual requirements.

Infrastructure which we have designed to be fault tolerant to a level that we determine given the nature of the systems. This means that the most important systems will have the highest levels of fault tolerance.

Procedures which have been adopted to minimise the exposure to an Information Security event, and to ensure that the impact of any such event is minimised.

Our Information Security management system covers not only the technical aspects of the provision of our service, but also the contractual and human resources aspects.

Information Security: a Partnership

We know that you want your Information kept secure. We also know that you want to be able to access your Information and process it with the minimum amount of fuss. That means that we have limited any requirements that are imposed on you as far as possible. However where you follow our guidelines (for example in your choice of password) you will be helping yourself to keep your Information secure.

Confidentiality Assured

Confidentiality is the aspect of Information Security that people think of most often, and that gets the largest headlines when there is a high-profile problem. We take a number of measures to ensure confidentiality including:

Customer Separation

Data for each customer is stored separately. This means that your business' Information is not held in the same database as another customers. (This is a notable difference to online banking, where all customers' Information is stored in the same database). Some services allow you to further protect your Information with passwords that you control if you choose.

Network Segregation

Internally our network is divided into segments that provide different services. This helps to minimise the ways in which your Information can be accessed.

User Authorisation

Access to our systems is by individually assigned user accounts which can be granted different levels of access. Passwords are validated against two separate systems. Before releasing or resetting user passwords we follow procedures to verify that the individual requesting the password is authorised to do so.

Scalable Redundant Infrastructure

One of the most effective ways to protect your Information is with an infrastructure that is designed to be highly available and reliable, minimising service outages and the possibility of data corruption.

Some of the measures we have adopted in our infrastructure are:

Load Balancing

Services are provided on multiple systems and users are directed to different systems according to availability and loading. The way the load is shared between the systems varies according to the nature of the service provided.

Redundant Routing

We connect to the rest of the Internet through a number of different ISPs (at the time of writing: NTT, Telia, Level(3) and Sprint). We are also a member of LINX (the London Internet Exchange) which allows us to connect directly to the networks of other members.

Failover clustering

Where appropriate services are provided using failover clustering where a system is on 'hot standby' to take over the operation of a service in the event that another system can no longer be used.

Distributed Clustering

Where appropriate services are provided on a collection of servers, with the service still being provided in the event of multiple failures in the underlying systems.

Are there ever any problems?

We cannot guarantee that a problem will never happen. Even with the most meticulous planning an unforeseen sequence of events can lead to an Information Security exposure. The ISO 27001 standard shows that we have a well thought out system to manage Information Security risks, to respond to events, to continually review and improve our performance and to communicate with users how we are doing.

For more information contact Online50:

Sales Desk:	0800 195 0835
Service Desk:	0870 855 5185
Web:	www.online50.net