Oxford Continuity Ltd.

The NextCloud
Business Continuity Server (UK)

In association with

■ HanssonIT (Sweden) https://www.hanssonit.se

■ ISO Standards: Advisera (Croatia) https://advisera.com

CONTACT
Oxford Continuity’s Managing Director

Paul Humphreys
paul@oxfordcontinuity.com
Kidlington ■ *Oxford* ■ *UK*

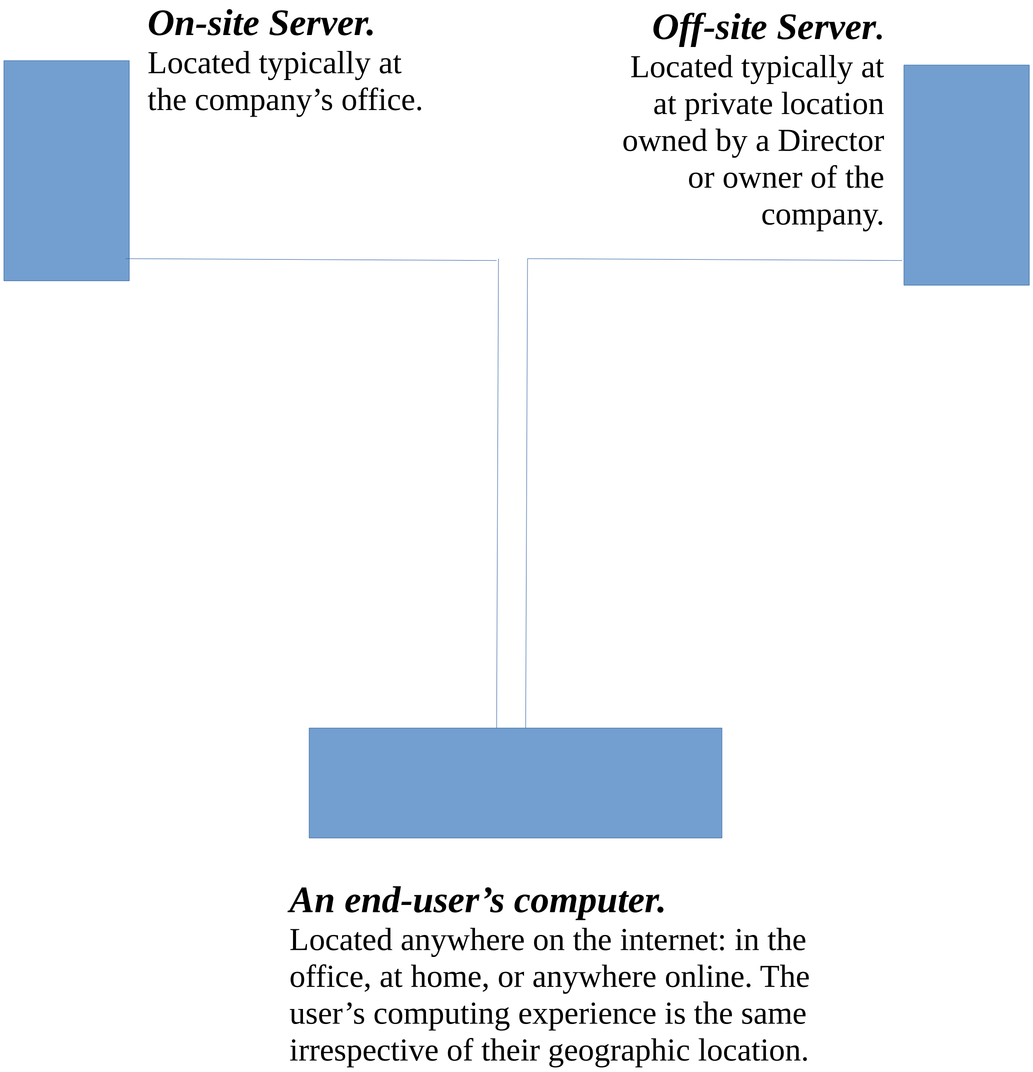
This Document Revision: January 2021

www.oxfordcontinuity.com

IDENTITY
OXFORD CONTINUITY LTD.
Founded 2001 ■ Established 2003
Company Number: GB-4940024
VAT Number: GB-795140318
Bank ID: HSBC 402631-81399284

GETTING UNDERWAY

An overview of the Oxford Business Continuity Network — with NextCloud software enabling *Data Sovereignty**



On-site Server.
Located typically at
the company's office.

Off-site Server.
Located typically at
at private location
owned by a Director
or owner of the
company.

An end-user's computer.
Located anywhere on the internet: in the
office, at home, or anywhere online. The
user's computing experience is the same
irrespective of their geographic location.

* Data sovereignty refers to the concept that data which an organisation collects, stores, and processes is subject to the nation's laws and general best practices where it is physically located. In the case of the Oxford Continuity Server, your data is stored on private servers wholly owned and controlled by you, housed in premises of your own choosing, and accessible only by users determined by you.

DEPLOYMENT POLICY

Business Continuity professionals know that even when Companies are armed with an excellent contingency plan — a plan long deliberated over by the firm's Directors, perfectly written and attaining the highest possible of marks when examined at the tabletop — businesses nevertheless can fail to recover within their plan's anticipated timeframe for one major reason: in peacetime, their plan has never been properly *rehearsed*. The disaster itself becomes the first opportunity for the plan to be *tested for real*.

Oxford Continuity's system is designed to ensure that core recovery practices are built-in from the outset forming natural contingency processes within normal day-to-day working routines exercised by all members of staff. These routines take on renewed importance from the year 2021 where organisations of all kinds are tending where practicable to move away from gathering in person at central offices but instead are migrating towards a *distributed* business model: *working from home and meeting online.*

This new way of working puts fresh focus on legacy contingency plans and a fresh emphasis on the concept of *distributed responsibility*. People have evacuated both the physical central office and *the office environment of daily disciplines.* In short, the Oxford Continuity model hands to each individual a greater personal share of the firm's collective responsibility to manage the security, backup, and recovery of those elements of business equipment and data over which individuals have immediate charge. These newly devolved responsibilities are no longer in the exclusive realm of central IT departments alone.

The Oxford Continuity model is designed to provide each individual user with the means at their own computer wherever located to ensure that their business data is managed safely, that their own designated files — including documents, calendars, lists of contacts and the like — are backed up to the agreed company schedule, and that each individual user knows independently *how to recover and continue* their own section of work, irrespective of what might come to befall any of their fellow workers. End-users of this system from Oxford Continuity are empowered to manage the backup and restoration of sets of data under their own immediate control, thereby dispersing data-resilience throughout the scope of the organisation while the Company retains central oversight of all its backup and recovery processes.

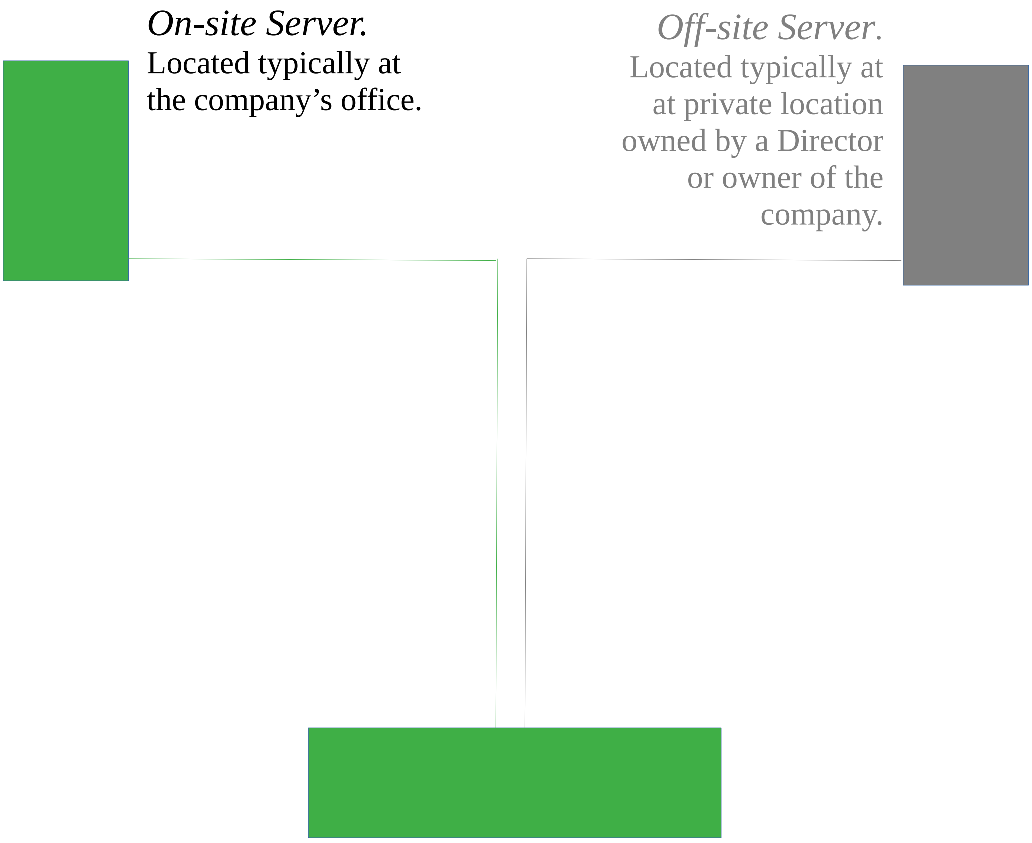
WHEN THE GOING’S GOOD

All users access the on-site server, all of the time.

The off-site server might never be used!

All is good — everything is safe and everyone is working well.

This diagram below perfectly expresses our target situation.



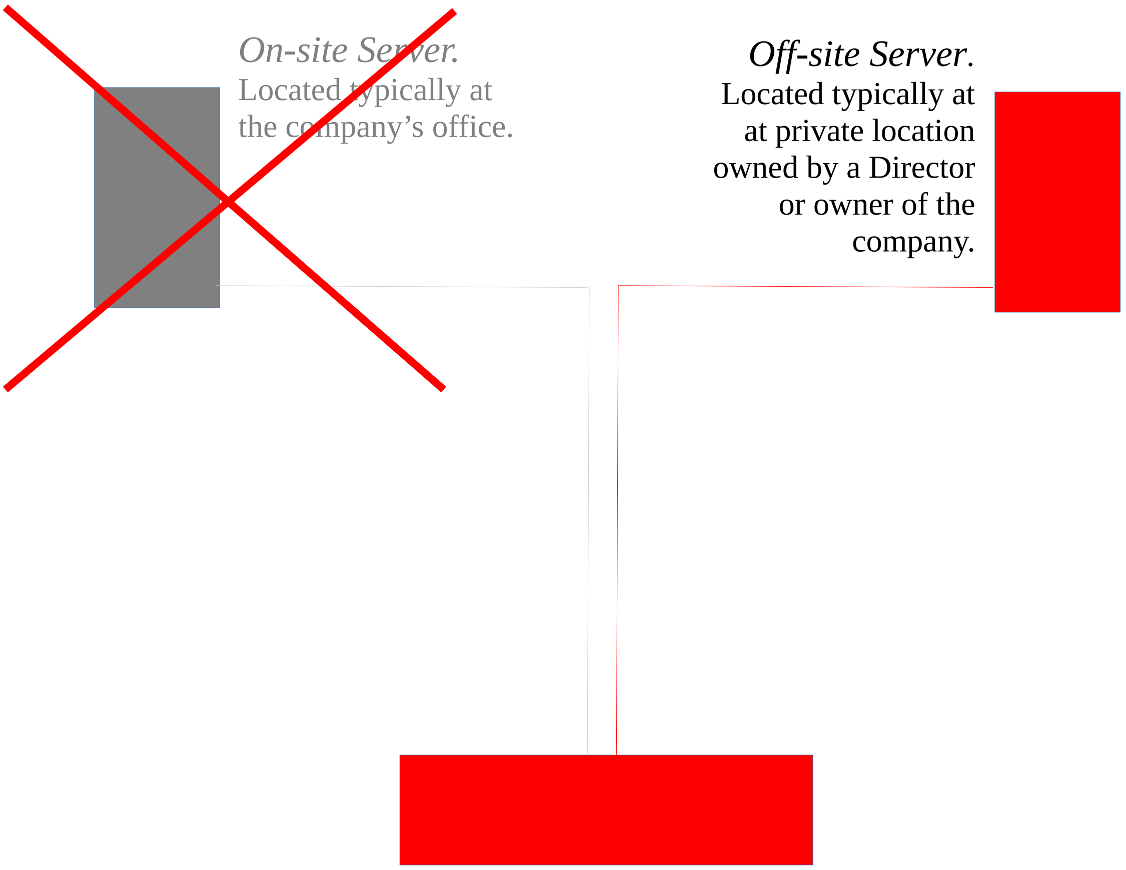
On-site Server.
Located typically at
the company’s office.

Off-site Server.
Located typically at
at private location
owned by a Director
or owner of the
company.

An end-user’s computer.
Located anywhere on the internet: in the office, at home, or anywhere online. The user’s computing experience is the same irrespective of their geographic location.

WHEN THINGS GO BADLY WRONG

When thing go badly wrong, users switch online to the off-site server
– until the disruptive situation on-site has been resolved.
Fire? Flood? Contamination? No local power supply? Loss of access to premises?



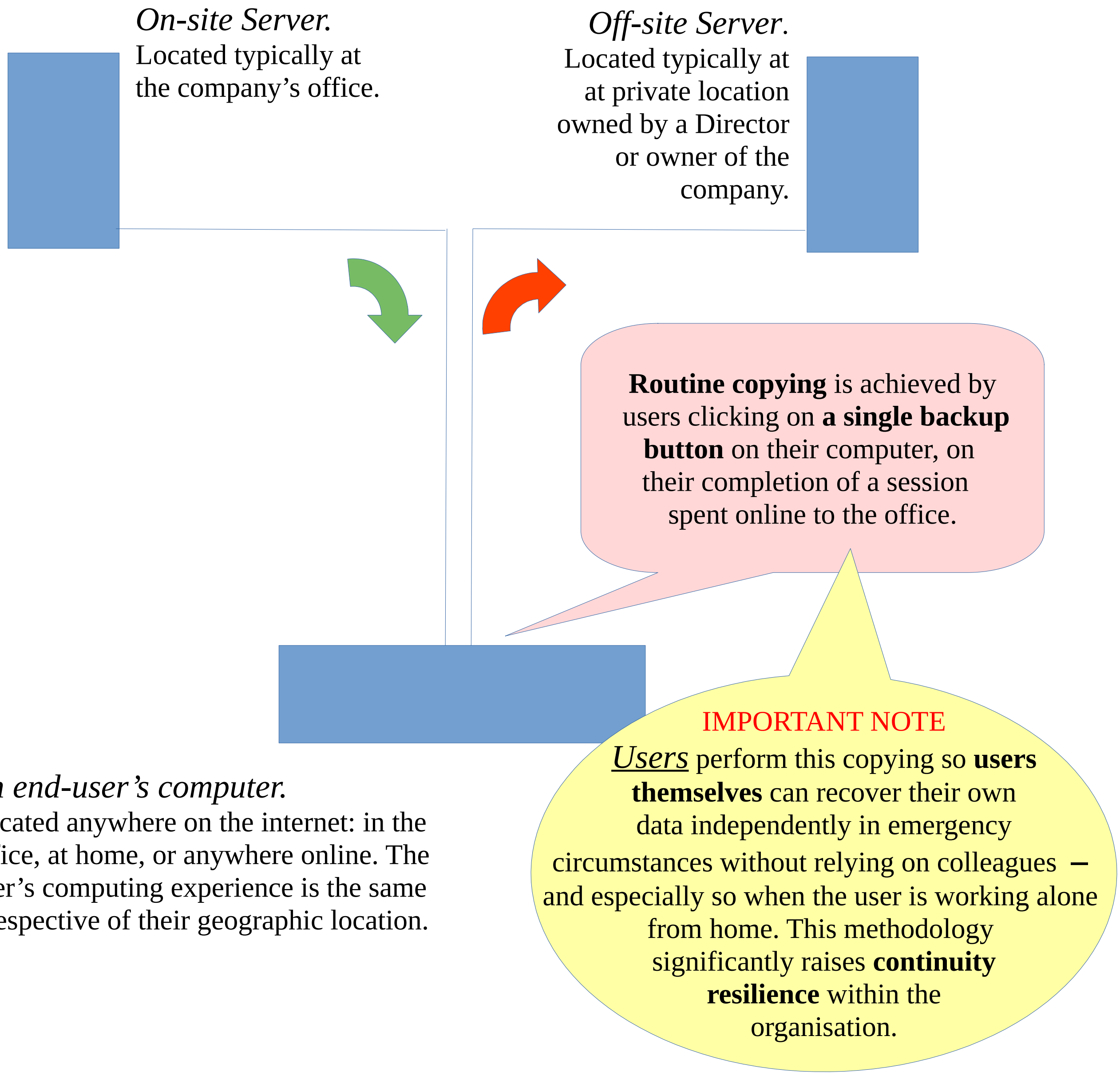
On-site Server.
Located typically at
the company's office.

Off-site Server.
Located typically at
at private location
owned by a Director
or owner of the
company.

An end-user's computer.
Located anywhere on the internet: in the office, at home, or anywhere online. The user's computing experience is the same irrespective of their geographic location.

WHAT’S HAPPENING IN THE BACKGROUND

Users routinely copy their own data from on-site to off-site.
This devolved backup process enables individual users in emergency circumstances to *recover* their own data from off-site and do so *independently from all other users*. ***In extremis***, an individual user *could* connect wholly to off-site while all other users remain on-site if available – but they should do so only in defined circumstances *as determined by Company policy*.



On-site Server.
Located typically at
the company’s office.

Off-site Server.
Located typically at
at private location
owned by a Director
or owner of the
company.

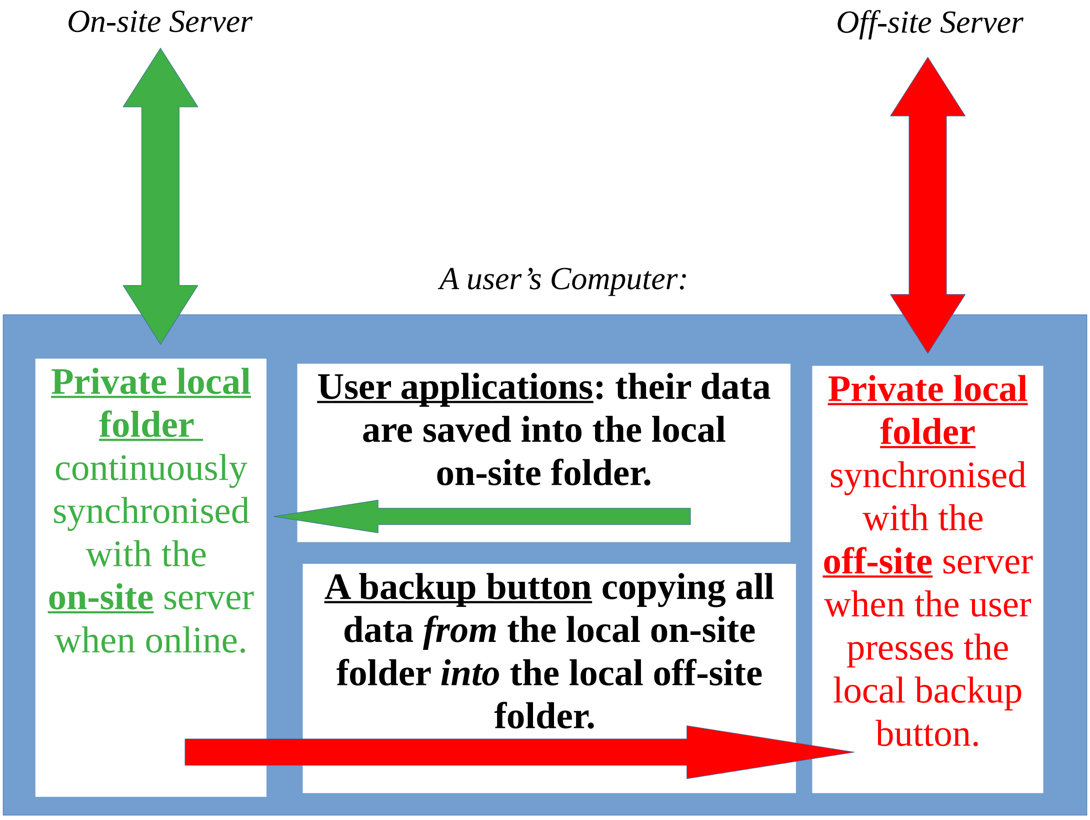
Routine copying is achieved by users clicking on **a single backup button** on their computer, on their completion of a session spent online to the office.

An end-user’s computer.
Located anywhere on the internet: in the office, at home, or anywhere online. The user’s computing experience is the same irrespective of their geographic location.

IMPORTANT NOTE
Users perform this copying so **users themselves** can recover their own data independently in emergency circumstances without relying on colleagues – and especially so when the user is working alone from home. This methodology significantly raises **continuity resilience** within the organisation.

A CLOSER LOOK INSIDE A USER'S COMPUTER

What's in the box?


On-site Server
Off-site Server
A user's Computer:
Private local folder continuously synchronised with the on-site server when online.
User applications: their data are saved into the local on-site folder.
A backup button copying all data from the local on-site folder into the local off-site folder.
Private local folder synchronised with the off-site server when the user presses the local backup button.

AN IMPORTANT NOTE ABOUT **USE OF EMAIL** ON THE USER'S PC

All emails received by the user are not automatically saved within the user's local on-site folder. We don't want to encourage untrusted or unnecessary emails to be routed directly into the heart of the primary on-site server. The user selects **only those emails of business value** (REF ISO: *information assets*) and explicitly copies those selected emails into their local designated folder from where they travel up the line and are saved inside the on-site server under controlled conditions, hence these relevant emails with their attachments may subsequently be shared **internally** with appropriate colleagues in the business. These *vitally important private information assets* should not be *forwarded* to colleagues using the *external* email system because that's deemed unsafe and insecure, and to do so would place the Company's business private correspondence at unnecessary risk of unauthorised exposure.

SEE ALSO
the article about Email Policy which follows.

EMAIL POLICY

Separation of | Message *Transmission* | from | Message *Storage*

When conceived, the electronic mail system was invented as a means of *transmitting* a message digitally from one person to another. And it worked.

As use of email grew, a convenient but insecure appendix was added at each end of the line to enable users to retain a copy of their messages sent and received. It is nowadays commonplace for users to utilise their email system as the primary *file-store* of their messages, indeed to do so has been encouraged along the way. Users are able to create folders and sub-folders to help them organise their messages within their email client application. The email system has morphed from a transmission system to become a *storage* system for what ISO today would refer to as being a vessel to hold a Company's *critical information assets.* Email is not the right vessel.

It is timely to rethink our use of email for business use in respect of data security.

Email messages ought to be filed as documents in folders held on the server.

For example, a user might receive ten email messages of which seven are of no business importance. Therefore, the user need file only three incoming messages in their internal storage system where subsequently they may be shared privately and *internally* within the Company. These three messages need not be left to languish within an essentially insecure public-facing email system.

Let us turn back the clock to the seconds following that very first and historic email message successfully sent and received. The recipient asks, "Is this message of significant importance to the work of my Company?". And if the answer is "Yes" only then should the receiver save that message into the firm's *private storage system* independent from the email transmission system through which the message arrived. The human recipient makes a vital judgement. The user act as an intelligent bridge between the external email system, and the Company's internal storage system.

Each email received is judged by its recipient: is this an *information asset* of importance to my Company? If it is, then I'll protect it — and I'll protect it now.

USER POLICY

Under Oxford Continuity’s methodology — **end-users take centre stage**.

An individual computer-user in normal circumstances may be working alongside colleagues seated at desks in rooms within the four walls of the firm’s central office; or the same user may be working from home or indeed from any internet-connected location anywhere in the world. In all cases, the user will fire up the firm’s preferred Internet browser to log-in to the Company’s instance of NextCloud where they enjoy *precisely the same data experience* from wherever they are connected to the Company’s primary Business Continuity Server. Geography and distance is immaterial in this respect.

As a reminder, Oxford Continuity’s Server system comprises *two* physical computers in a server role: one machine designated the *on-site server* typically is located at the firm’s central office. This *primary server* is the twin to which *all users* in the Company routinely connect from both inside and outside the office. Users inside the office connect via their ethernet-wired local area network; users from outside connect to the same server over their current location’s local Internet service from where all data in transit is encrypted between the user’s computer and the on-site server. The second twin is designated the *off-site server* and, with good fortune, *it may never come to be used* in full replacement of its primary twin. Vitally, the secondary is located at *a different private location* to which users connect *in extremis* as determined by Company policy. The role of the secondary server is to be on permanent active standby for immediate switch-to by users should the primary server become unavailable however caused. Importantly, although continuously on standby, users should not attempt to connect to the off-site server unless instructed by policy to do so: because the primary server may only briefly become unavailable for known and controlled reasons, and so, albeit possibly inconvenient for some current users, on-site may very shortly return to service. But users must always *remain aware of this contingency plan* and be prepared quickly to switch to it. Indeed, users are rehearsed in making this switch under controlled conditions simulating emergency circumstances. But equally so, a war simulation unexpectedly may be called!

That reminder made, each user is given a simple means to copy their own set of data held on the on-site server, with know-how to retrieve it from the off-site server from where their applications await continued access in exceptional — otherwise disruptive — circumstances.

ABOUT BEST PRACTICE

Implementing the recommendations of the International Standards Organisation (ISO) in Information Security.

Oxford Continuity is especially grateful for its association with **Advisera** for creating an online information system which **makes Standards easy to understand and simple to implement**. And so we advise you as a client or prospective client of Oxford Continuity to sign-up today for Advisera's free introductory resources. You'll quickly learn how to apply important methodologies in your own daily routines for all kinds of computing purposes, but especially those concerned with your day-to-day business operations.

We especially encourage those of you who are owners and Directors of companies to consider working towards *formal certification* of your Company in the appropriate ISO Standards for your business sector, and for which Advisera has ample resources to help you explore some apparently complex issues in depth while you consider what's involved in the accreditation process — including better understanding of the *business advantages* for your firm by achieving official certification.

There's no need to wait beyond today. Right now you can visit Advisera and sign up today for some free online tuition and get started straightaway. Or assign this exploratory task to a member of your team.

To get ahead with your understanding of the application of International Standards in your own organisation visit https://www.advisera.com. Do this especially if you intend to adopt the Oxford Continuity system.

Here's a good practical example of what's on offer.

There are many elements involved in implementing the ISO 27001 standard in Information Security. **For example:** the Standard's criterion for ***use of strong passwords*** is something advised for all business users. For your Company quickly to enforce this particular policy, the means to do so is already included within the NextCloud system. You'll find a simple tick-box asking whether or not your Company wishes to enforce the use of strong passwords for all its users. If you do, then simply ***tick the box, and you're done.*** And you'll have made your first big step towards achieving your own Company's ISO certificate. But with Oxford Continuity it's not *entirely* all ready for you out of the box. There's plenty of study and practice ahead – for you and your colleagues – as you work towards your final exam.