Prefect

Cleverly simple
control of energy.

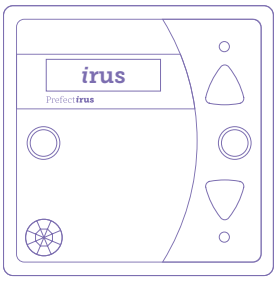
Prefect Irus **Security and Resilience**

V3 - 01/2024

irus

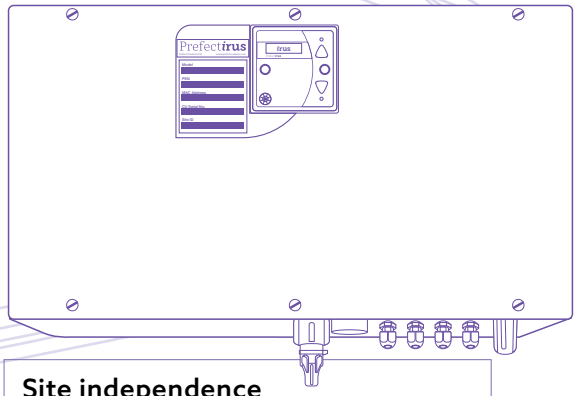
Resilience

The Irus system is designed to tolerate equipment or network failure, with each part of the system able to operate independently if necessary:



Node fall-back

Every unit on a site is configured with 'fall-back' behaviour which is activated after an extended period without communication from the mIFU. This ensures that site residents still have heating and hot water even in the event of a mIFU break-down.



Site independence

Site independence – The mIFU can run indefinitely without a connection to the Irus Portal. Schedules will operate as normal, and data will be logged until communication with the Portal is re-established.

Irus Portal

Irus Portal – The Portal is hosted in a UK-based Microsoft Azure datacentre with multiple levels of redundancy for power and network connections. If the equipment running the portal were to fail, the workload would be automatically switched to new hardware within the datacentre.

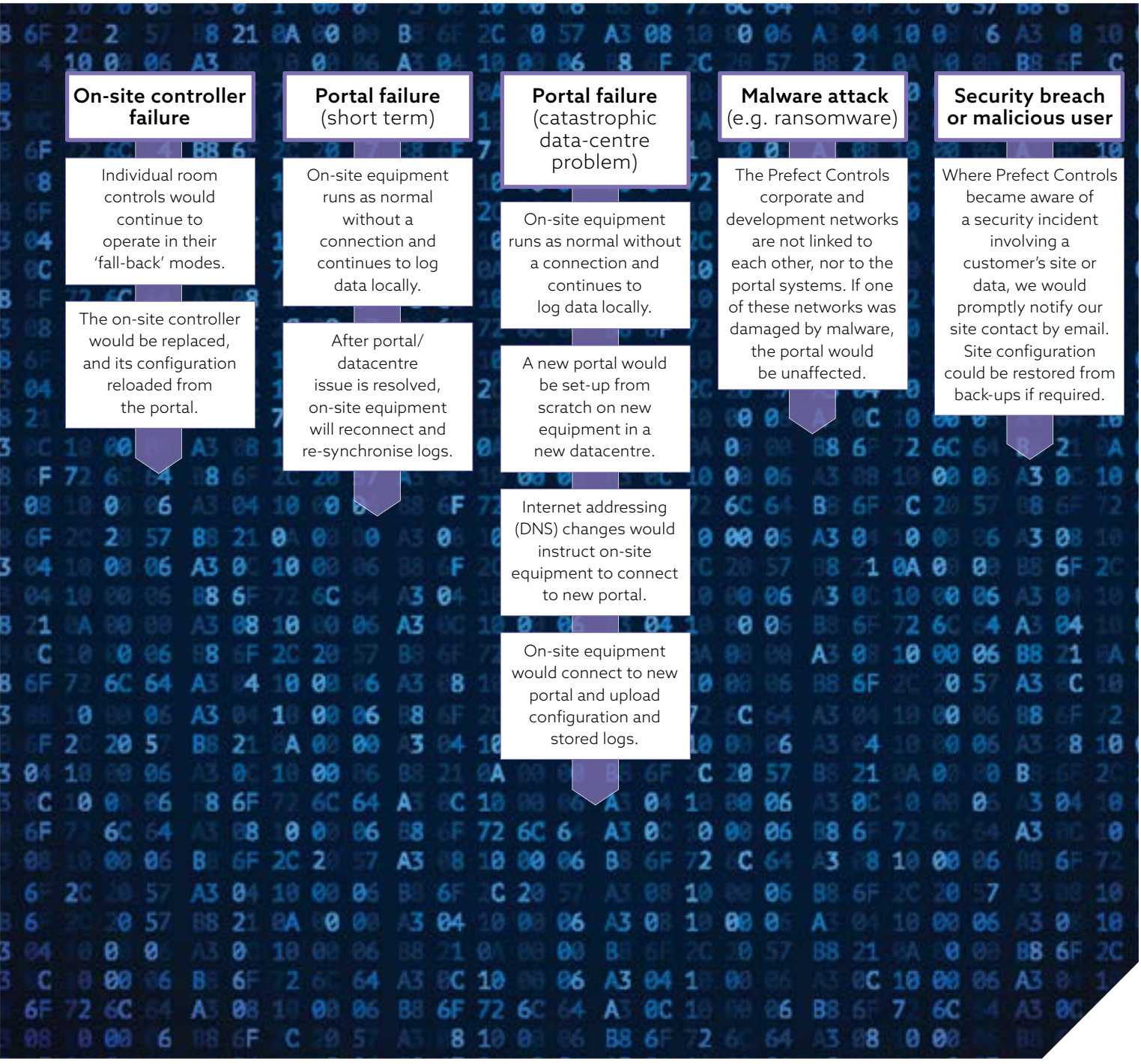
Data storage

Data Storage – Log data is collected every 10 minutes from each site and stored at the Portal within Azure Storage. Other portal management information is stored within a separate database hosted within Azure which is continuously backed-up. These backups are retained for 14 days and can be restored via the Azure management tools if necessary.

Additionally, all site-specific configuration information (needed for the prompt restoration of a mIFU) is archived at Prefect Controls premises every day. This data is retained indefinitely.

Incident recovery

Some examples of potential incidents and their recovery processes:



irus

Security

On-site equipment

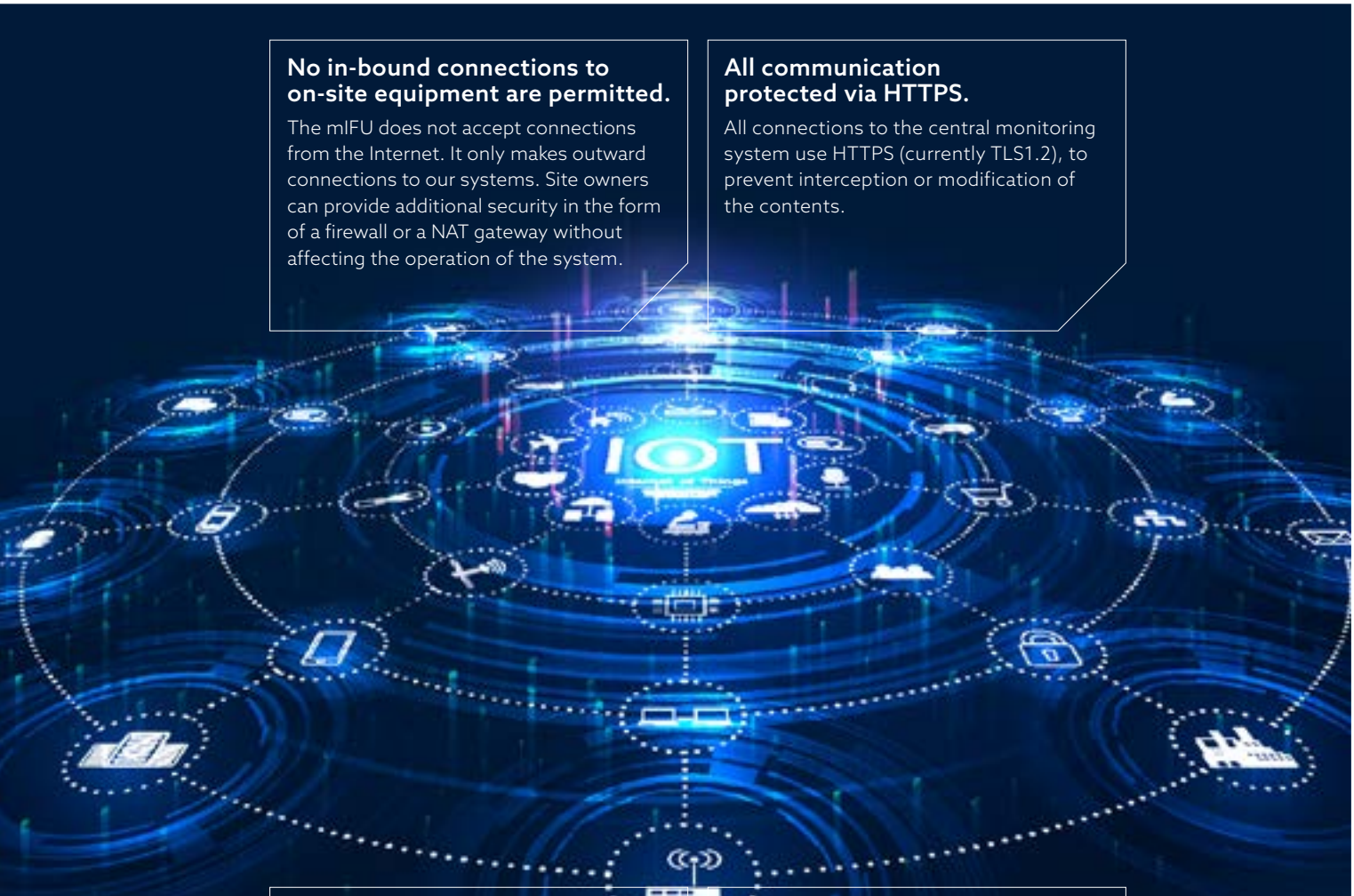
The Irus site controller (“mIFU”) communicates with the Irus Portal via the Internet. In order to maximise the security of this link, the following measures apply:

No in-bound connections to on-site equipment are permitted.

The mIFU does not accept connections from the Internet. It only makes outward connections to our systems. Site owners can provide additional security in the form of a firewall or a NAT gateway without affecting the operation of the system.

All communication protected via HTTPS.

All connections to the central monitoring system use HTTPS (currently TLS1.2), to prevent interception or modification of the contents.



mIFU authorisation.

A specific mIFU must be authorised to connect to the Irus Portal.
An attempt to connect an unauthorised mIFU will be rejected and the system operators notified.

Physical security.

There are no maintenance ports on the exterior of the IFU. The connection of maintenance equipment requires the removal (using tools) of the front panel. It is the site owner’s responsibility to ensure that there is no unauthorised access to the IFU.

Central site

The central monitoring system is hosted by Prefect Controls within a Microsoft Azure datacentre. It monitors and archives data from multiple sites, and access to the data and control of each site is restricted by user accounts. The following security measures apply:

HTTPS-protected access.

To prevent the interception of confidential information or security tokens, all access to the system uses the HTTPS (currently TLS1.2) protocol.

Single sign-on.

The Irus Portal is designed to integrate with a customer's existing log-in system, which avoids users needing new accounts or passwords specifically for use with the Portal. This is our recommended approach. (See details below)

Secure password storage

Where single sign-on cannot be used, we do offer password protected accounts. Passwords are stored securely in our system using a salted PBKDF2 hash (RFC2898).

Master/backdoor accounts

Master / backdoor accounts – as part of our monitoring service, Prefect Controls do require access to all sites. This is performed using named individual user accounts, that have been granted the appropriate level of access. There is no master account or maintenance back-door which could be exploited. All Prefect Controls users are required to use two-factor authentication.

Physical security

The Microsoft Azure datacentres have robust physical security, subject to extensive 3rd-party audit. Some details - https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Firewalling

The components of the portal within the datacentre are configured with restricted access, such that only the Prefect Controls development network can connect to them. Other external access is not permitted.

User management tools

At a customer's request, Prefect can designate one or more users as "User Managers", who are able to configure their colleagues' access permissions.

Security audit

Prefect Controls run a variety of 3rd-party security audit tools against the Irus Portal to ensure that the Portal is maintained according to industry best-practices.

irus

Security

Single sign-on

We strongly recommend that customers chose to integrate the Irus Portal with their organisation's existing log-in system. This offers many advantages:

Ease-of-use

Users will not need to remember (or write down) yet another set of credentials – they can use all the same details that they use for other systems, and in many cases their web-browsers will already know this information, so signing-in to the Prefect Irus system is seamless.

Central control of security policy

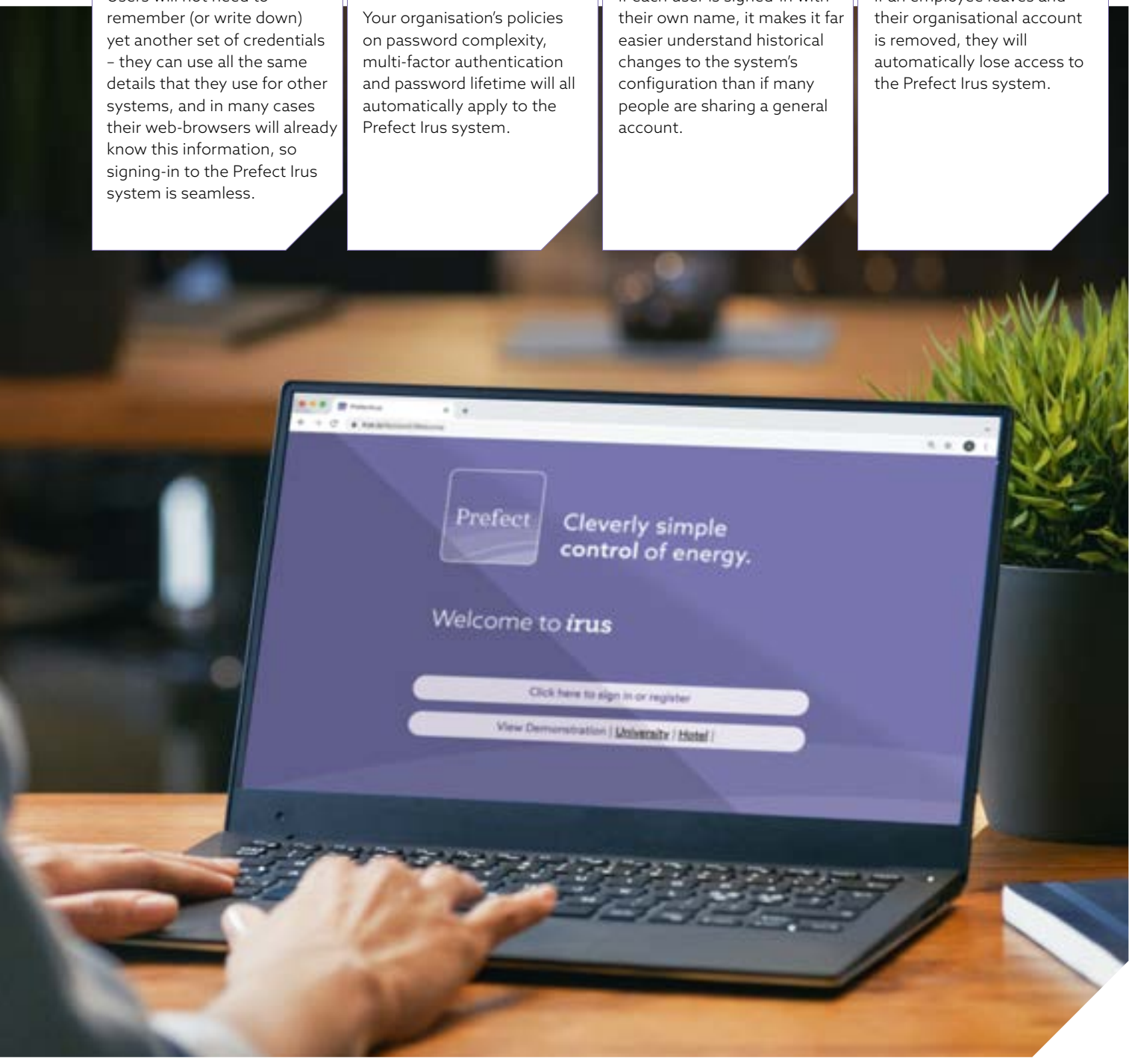
Your organisation's policies on password complexity, multi-factor authentication and password lifetime will all automatically apply to the Prefect Irus system.

Accountability

If each user is signed-in with their own name, it makes it far easier understand historical changes to the system's configuration than if many people are sharing a general account.

Account revocation

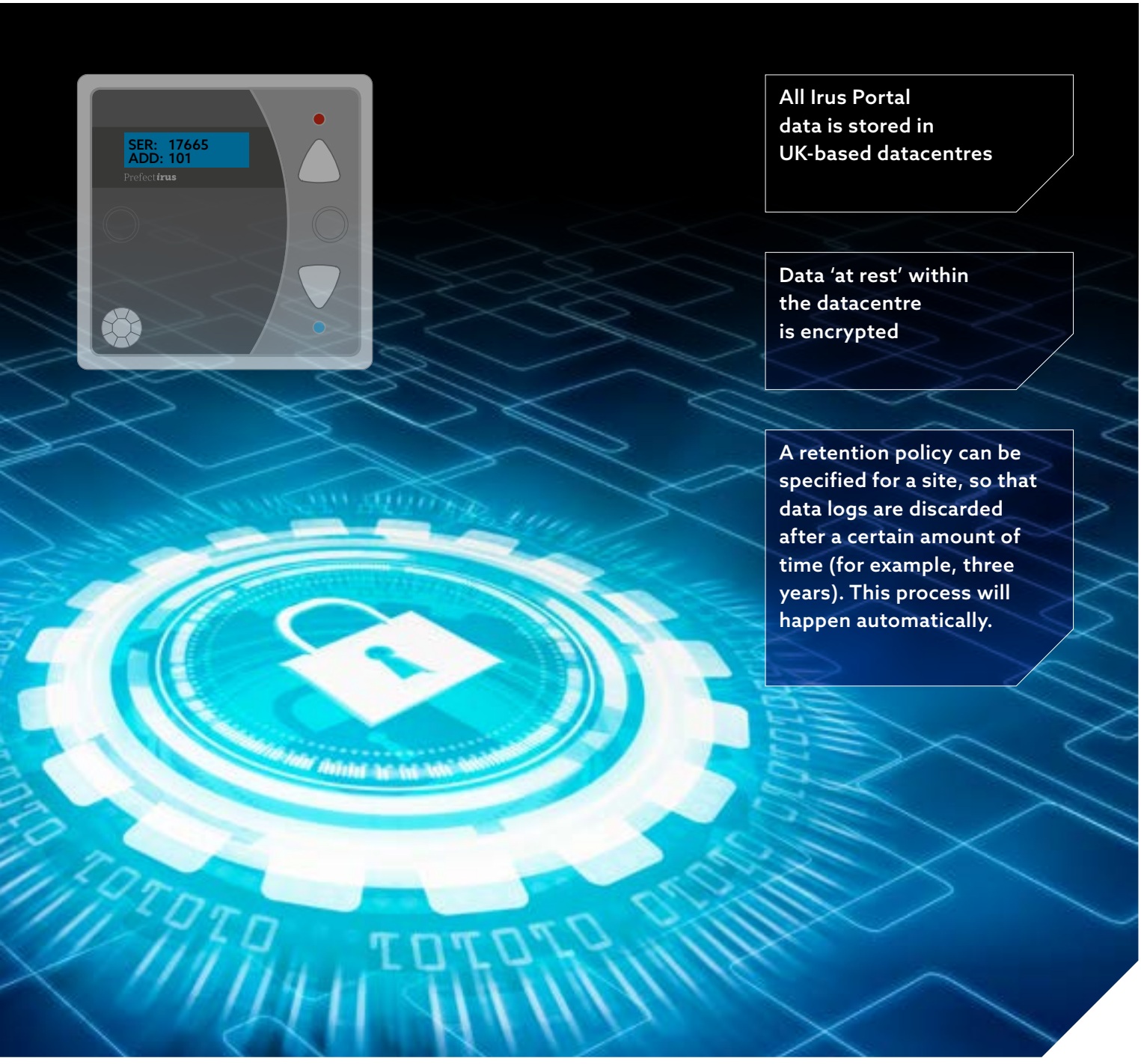
If an employee leaves and their organisational account is removed, they will automatically lose access to the Prefect Irus system.



Data handling

The Irus Portal records and stores environmental data from its various sensors. This data is stored by reference to the numerical address of the sensor from which it was obtained and is not "personal data" for the purposes of data protection regulations.

However, customers may be able to use other systems to combine the identity of individuals with data stored on the Prefect Portal, and they may wish to control access to such data. To assist with this access control, each Portal user may be restricted as to the number of days of history they are able to view for each room.



Prefect

Cleverly simple
control of energy.

Prefectcontrols.com

Prefect Controls Limited, Unit 2 Church Field Business Park, Church Field Road, Sudbury, Suffolk CO10 2YF
T: 01787 320604 | E: mail@prefectcontrols.com

10453 V3