OREGA REGULATED CONNECTIVITY WHITE PAPER

Enterprise Connectivity and Security for FCA-Regulated Businesses

Flexible infrastructure aligned to compliance, control and operational performance requirements

Executive Summary

FCA-regulated and security-conscious businesses need more than internet access. They require reliable connectivity, clear network segregation, strong security boundaries, auditability and a practical operating model that aligns with their internal policies, regulatory obligations and client assurance requirements.

Orega's workspace infrastructure is designed to support these requirements from day one. Each centre is built on enterprise-grade connectivity, managed switching, secure Wi-Fi and resilient network architecture. For most regulated businesses, this provides a secure and operationally efficient platform without the need to deploy and manage separate physical infrastructure.

Where a client requires additional control, Orega can support defined models that increase client ownership of the firewall, routing and internal network environment, while maintaining appropriate control over the shared building infrastructure. This is particularly important in multi-tenanted buildings, where unmanaged client Wi-Fi or duplicate access infrastructure can reduce performance, increase interference and create wider operational risk.

The core principle is simple: Orega can provide secure, managed access infrastructure, while the client retains control of its own security boundary where required.

1. Enterprise Connectivity by Default

Every Orega centre is designed to support modern business operations, including cloud services, video conferencing, secure remote access, collaboration platforms and regulated-client workloads.

Orega's standard infrastructure typically includes:

- Private company networks using VLAN segregation
- High-capacity fibre connectivity
- Managed switching across the building
- Managed Wi-Fi across the centre
- Enterprise firewall protection
- Resilient connectivity and monitoring
- Professionally managed network infrastructure

This allows clients to move in and operate securely without immediately needing to procure, install and support their own infrastructure.

For many businesses, including many FCA-regulated firms, Orega's standard model provides the right balance of security, speed, resilience and operational simplicity.

2. Requirements of Regulated and Security-Conscious Clients

Orega supports a wide range of FCA-regulated firms, financial services organisations, professional services businesses and security-conscious occupiers.

Common requirements include:

- Secure separation from other occupiers
- Control over firewall and security policies
- Defined network boundaries
- Support for audit and vendor assurance processes
- Alignment with internal IT standards
- Reliable connectivity and resilient service design
- The ability to evidence appropriate technical and organisational controls

Some clients also have global IT policies, client contractual obligations or audit frameworks that require them to demonstrate direct control over certain elements of their network environment.

Orega's model is designed to support these requirements through clearly defined service options, with increasing levels of client control where needed.

3. Service Models: Increasing Control, Complexity and Cost

Orega offers a range of connectivity models. These are designed to provide flexibility while preserving the integrity and performance of the shared building environment.

3.1 Standard: Fully Managed

Under the standard model, Orega provides and manages the core network environment.

This typically includes:

- Orega-managed firewall
- Orega-managed switching
- Orega-managed Wi-Fi
- Private company VLAN

- Secure, plug-and-play access

This model is suitable for most clients who require secure connectivity without the complexity of managing their own network infrastructure.

3.2 Client Firewall: Enhanced Client Control

For clients requiring direct control over their security policies and boundary device, Orega can provide a clean handoff to a client-managed firewall or router.

This model typically includes:

- Client-managed firewall or router
- Public IP provision where required
- Orega-managed switching and Wi-Fi
- Dedicated client VLAN
- Clear demarcation between Orega infrastructure and client-controlled security environment

This is often the preferred model for regulated clients. The client controls the firewall, routing, security policy, logging, filtering and onward connectivity, while Orega continues to manage the building infrastructure.

3.3 Wires Only: Controlled Exception

Where a client requires further control, Orega may support a model where the client operates its own firewall and switching environment, with Orega providing connectivity and agreed handoff points.

This model may include:

- Client-managed firewall
- Client-managed switching within an agreed scope
- Orega connectivity
- Orega-managed Wi-Fi where appropriate
- Defined patching and demarcation arrangements

This model is more complex and must be agreed in advance. It may involve additional installation, patching, labelling and reinstatement requirements.

3.4 Wires Only plus Client Wi-Fi: Exceptional or Air-Gapped Requirement Only

Client-installed Wi-Fi is not Orega's preferred model in a multi-tenanted environment. It may be considered only where there is a specific technical, contractual or compliance requirement that cannot be satisfied through Orega-managed Wi-Fi and VLAN presentation.

Where approved, client Wi-Fi would normally be subject to strict guardrails, including:

- In-suite deployment only
- Agreed access point locations
- Low power operation
- 2.4GHz disabled unless expressly agreed
- Coordination with Orega and its network provider
- No adverse impact on the wider building RF environment
- Full reinstatement on exit

This model provides maximum client control but also introduces greater complexity, cost and potential impact on the shared wireless environment.

4. Wi-Fi Strategy in a Multi-Tenanted Building

Wi-Fi is a shared radio environment. Unlike a physical cable, wireless spectrum is used by all nearby networks and devices. Poorly configured or unmanaged access points can create interference, reduce capacity and degrade performance for multiple occupiers.

For this reason, Orega manages Wi-Fi at building level.

A coordinated building-wide Wi-Fi design allows Orega to:

- Manage channel allocation
- Reduce RF interference
- Control access point power levels
- Maintain consistent coverage
- Protect performance for all occupiers
- Avoid unnecessary duplication of wireless networks
- Monitor and troubleshoot the environment more effectively

A single client-installed access point inside a suite will often underperform compared with a coordinated building-wide Wi-Fi system. It can also negatively affect neighbouring clients by creating additional channel contention and RF noise.

In dense urban buildings, especially multi-tenanted workspaces, more Wi-Fi equipment does not necessarily mean better Wi-Fi. In many cases, it creates the opposite outcome.

5. Wi-Fi as a Secure Access Transport Layer

A key point for regulated clients is that Wi-Fi does not need to be the client's security boundary.

In Orega's managed model, Wi-Fi can act as an access transport layer, similar to structured cabling, a patch panel or an Ethernet wall port.

For example, where Orega presents a dedicated client VLAN to a physical data port, the client does not own the building cabling, riser, patch panel or Orega switch. However, the client's traffic can still be logically segregated and delivered into the client's own firewall or router.

The same principle can apply to managed Wi-Fi.

A user can connect to the common Orega Wi-Fi SSID using client-specific credentials or a client-specific PSK. Those credentials can map the user's traffic into the client's dedicated VLAN. The traffic is then routed to the client's own firewall or security boundary.

In this model:

- Orega manages the Wi-Fi access layer and RF environment
- The client's traffic is logically segregated into a dedicated VLAN
- The client's firewall or router remains the managed security boundary
- The client retains control of routing, security policy and onward connectivity
- Users can access the client network from agreed areas of the centre
- Additional client access points are avoided

This approach allows a client to maintain network segregation and control of its security boundary without needing to install and manage separate Wi-Fi infrastructure.

6. Supporting Client Security Requirements

Orega's model is designed to support common regulated-client requirements by separating the access infrastructure from the client-controlled security boundary.

Logical access controls

Client traffic can be segregated into a dedicated VLAN and delivered to the client's own firewall or router.

Network boundary management

Where required, the client's firewall or router remains the boundary device under the client's administrative control. The client can manage routing, filtering, VPN, logging, policy enforcement and onward connectivity.

Dedicated and segregated infrastructure requirements

Dedicated logical infrastructure can be provided without requiring the client to own every physical component in the access path. This is similar to using a dedicated VLAN over Orega-managed cabling, patching and switching.

Information flow enforcement

Information flow can be enforced at the client firewall or router, while Orega-managed cabling, switching and Wi-Fi provide the access layer.

Auditability

Where required, client-specific credentials, user authentication, VLAN assignment and firewall logging can support the client's audit and assurance processes.

Multi-tenanted building control

Orega retains management of the shared RF environment and building infrastructure to protect performance, capacity and security for all occupiers.

7. Authentication Options

Orega can support different authentication models depending on client requirements and the technical design agreed for the site.

Client-Specific PSK or Credential Mapping

A client-specific password, credential or PSK can map authorised users into the client's dedicated VLAN over the common Orega SSID.

This approach avoids broadcasting multiple client-specific SSIDs while maintaining logical separation between client networks.

Benefits include:

- Simple user experience
- Reduced Wi-Fi network clutter
- Logical segregation through VLAN assignment
- Better RF management
- Easier support across the building

Individual User Login

Where required, per-user authentication can provide stronger access control and auditability.

Benefits include:

- Individual user accountability
- Easier access revocation

- Better audit trail
- Improved alignment with regulated-client requirements

The appropriate authentication model should be agreed as part of the client's technical scope.

8. Client-Owned Wi-Fi: Exception Only

Client-owned Wi-Fi may be considered only where there is a specific requirement that cannot be met through Orega-managed Wi-Fi and VLAN presentation.

This is because unmanaged or additional access points can:

- Increase RF interference
- Reduce available channel capacity
- Degrade performance for the client and neighbouring occupiers
- Create troubleshooting complexity
- Undermine building-wide Wi-Fi design
- Increase operational and compliance risk in shared areas

Where client Wi-Fi is approved, it must be deployed within defined conditions and remain subject to Orega approval.

Typical conditions include:

- In-suite access points only
- No use in shared or common areas
- Low power settings
- 2.4GHz disabled unless agreed
- Agreed channels and configuration
- No interference with Orega-managed Wi-Fi
- Installation by or in coordination with Orega's nominated provider
- Full reinstatement on exit

This model should be treated as a controlled exception, not the standard approach.

9. Infrastructure, Installation and Demarcation

Where client equipment is introduced, the technical scope must be agreed before installation.

This should include:

- Required rack space
- Firewall/router model
- Switch count and model
- Power requirements
- Public IP requirements
- VLAN requirements
- DHCP approach
- Inter-suite connectivity requirements
- Patching requirements
- Support responsibilities
- Decommissioning and reinstatement obligations

All comms room work, patching, repatching, labelling and reinstatement must be coordinated by Orega and its nominated network provider.

Additional charges may apply for installation, patching, labelling, decommissioning and reinstatement.

A clear demarcation of responsibility must be maintained at all times.

10. Responsibility Model

Orega is typically responsible for:

- Building connectivity platform
- Core network infrastructure
- Managed switching, where applicable
- Managed Wi-Fi and RF environment
- Cabling and patching infrastructure
- Comms room governance
- Monitoring and management of Orega infrastructure

The client is typically responsible for:

- Client firewall or router, where applicable
- Client security policies
- Client routing and filtering
- VPN and remote access services

- Internal network configuration in exception models
- End-user devices
- Client applications and data
- Compliance of client-managed infrastructure

This separation allows clients to evidence control over their own security boundary while allowing Orega to protect the integrity of the shared building infrastructure.

11. Fully Segregated or Air-Gapped Environments

In some circumstances, a client may require a fully segregated or air-gapped environment with minimal reliance on shared infrastructure.

Where required and technically feasible, Orega may support:

- Client-operated firewall
- Client-operated switching
- Client-operated Wi-Fi, subject to approval
- Connectivity provided as handoff only
- Separate installation, patching and reinstatement arrangements

This is a controlled exception and will usually involve additional cost, longer lead times, more complex operational arrangements and stricter approval conditions.

12. Why Regulated Businesses Choose Orega

Regulated and security-conscious businesses choose Orega because the platform offers both security and flexibility.

Key benefits include:

- Enterprise-grade connectivity
- Secure private company networks
- Managed Wi-Fi across the building
- Clear options for client-managed firewalls
- Support for regulated-client assurance requirements
- Scalable service models
- Defined responsibility and demarcation
- Practical balance between control, cost and complexity

- Protection of the shared multi-tenanted environment

Orega's approach allows clients to increase control where genuinely required, without defaulting to unnecessary duplication of infrastructure.

13. Conclusion

Orega provides secure, resilient and enterprise-grade connectivity as standard.

For FCA-regulated and security-conscious clients, Orega can support additional control through defined models that allow the client to manage its own firewall, routing, security policies and network boundary.

In many cases, the most effective solution is not for the client to install its own Wi-Fi access points, but for Orega to present the client's dedicated VLAN over the managed Orega Wi-Fi infrastructure. In that model, Wi-Fi acts as a secure access transport layer, while the client retains control of its security boundary.

This provides a practical balance of security, performance, auditability and operational control.

Secure by default. Flexible where required. Controlled where necessary.