CUSTOMER DOCUMENTATION SAMPLE

Environment As Built and Systems Map

Logical record of cloud services site infrastructure data flows and operating dependencies

Prepared for Harborlight Design Studio | Fictional demonstration environment

This document records the sample environment as it is represented on the evidence date. It explains the role of each major component and the dependencies that matter to support and recovery. Exact customer identifiers and privileged configuration are intentionally omitted from the public sample.

Document Control

CLASSIFICATION	Public fictional sample	VERSION	1.0
DOCUMENT OWNER	Tyler's Tech Company	EVIDENCE DATE	September 5 2026
REVIEW CADENCE	Quarterly and after material change	SAMPLE STATUS	Public fictional example

How to read status labels Verified, Customer confirmed, Provider reported, Planned, Out of scope, and Not verified show how evidence would be classified in a live customer document. All facts and statuses in this public sample are fictional.

Scope and Evidence

Evidence source	What it supports	Sample status
Administrative inventory	Covered users devices Microsoft 365 services and backup jobs	Verified
Network controller readback	Firewall switching and wireless device roles	Verified
Customer operations interview	Business application ownership priority and workflow	Customer confirmed
Provider portals	Internet service and cloud platform status	Provider reported
Public sample sanitization	Removal of detailed identifiers endpoints credentials and exploitable configuration	Applied

Business Data Flow

Email and shared working files remain in Microsoft 365. Project and finance records remain in their approved business services. Design work requiring workstation backup is included only for specifically enrolled folders and devices. Synchronization inside a service is not treated as an independent backup unless a separate recovery copy exists and has been tested.

Logical Systems Map

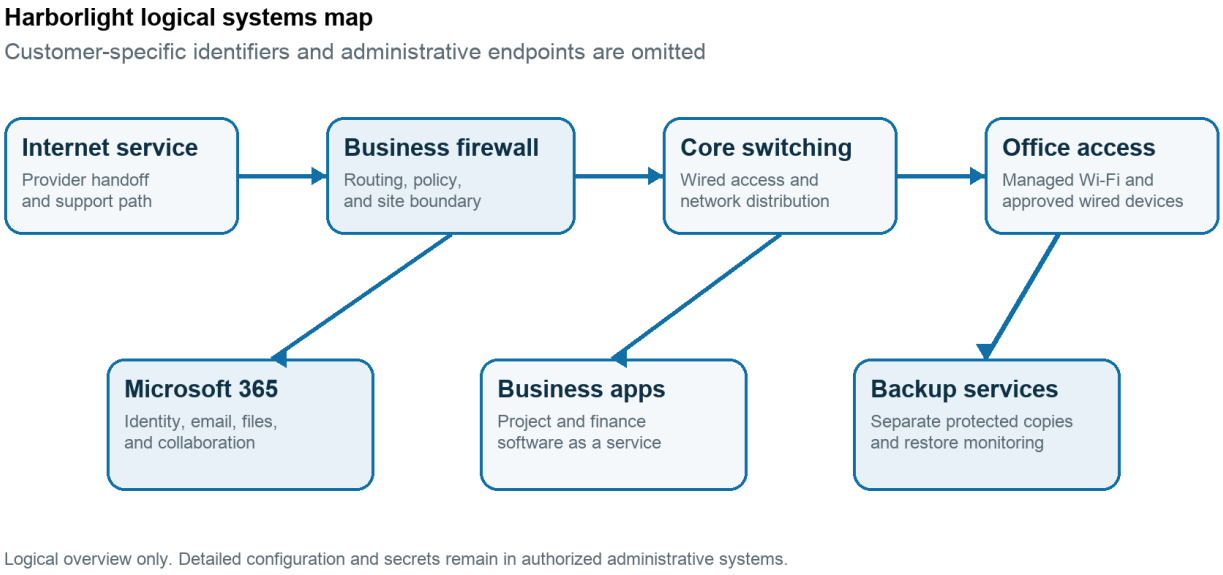

Figure 1 Logical relationship view for the fictional Harborlight environment

How to read the map. Office traffic reaches the managed site boundary before switching and approved access. Managed devices use approved identity and internet access for cloud services. Backup services protect only the workloads listed in the recovery plan, and successful jobs still require restore testing.

Component Roles

Component	Role	Management boundary	Dependency
Internet provider handoff	Primary office connectivity	Provider circuit with TTCo coordination	Provider network and customer power
Business firewall	Site boundary routing and network policy	TTCo managed within approved scope	Provider handoff and current configuration backup
Core switching	Connects wired infrastructure and access points	TTCo managed	Firewall uplink and stable power
Managed Wi-Fi	Employee and approved guest wireless access	TTCo managed policy and equipment	Switching authentication and radio coverage
Microsoft 365	Identity email files and collaboration	TTCo administration with customer approval	Internet access identity configuration and Microsoft service
Business applications	Project and finance workflows	Customer and vendor owned with TTCo coordination	Identity vendor availability and business ownership
Backup services	Separate protected copies for covered data	TTCo monitoring with customer recovery authorization	Source access storage service and recovery credentials

Identity and Access Flow

1. An authorized Harborlight contact approves the employee event and required business role.
2. TTCo administers covered identity groups applications and device enrollment using named administrative access.
3. The employee signs in with an individual account and the approved multifactor method.
4. Applications receive access through assigned licensing group membership or a documented vendor process.
5. Role changes and departures update the employee lifecycle record and retain completion evidence.

Monitoring and Resilience

Area	Observed or reported control	Review signal	Status
Internet	Provider service plus documented escalation path	Circuit availability and provider incident	Provider reported
Site power	Battery backup for firewall switching and access points	Runtime self-test and battery age	Verified
Network configuration	Controller-managed configuration with protected administrative access	Configuration change and device health	Verified
Microsoft 365	Service health and separate covered-data backup	Service incident backup job and restore test	Provider reported
Endpoints	Managed policy security tooling and replacement process	Check-in protection status and lifecycle	Verified
Business applications	Vendor-hosted availability and customer-owned procedures	Vendor status and customer escalation	Not verified

Known Limitations and Exclusions

- The public map is logical. It does not include exact network segments, addresses, radio settings, firewall rules, serial numbers, floor plans, or management endpoints.
- Home networks, personally owned devices, and unsupported building systems are outside scope.
- Vendor-hosted application resilience is provider reported unless a separate recovery test is recorded.
- A source inventory or green dashboard does not prove that a full business process can be recovered.

Update Triggers

Update this record after a site or provider change, material network change, new core application, backup coverage change, identity-platform change, or completed project that changes a dependency. Record the evidence date and approver when the update affects operating responsibility.

Revision History

Version	Date	Change	Prepared by
1.0	September 2026	Public sample release	Tyler's Tech Company