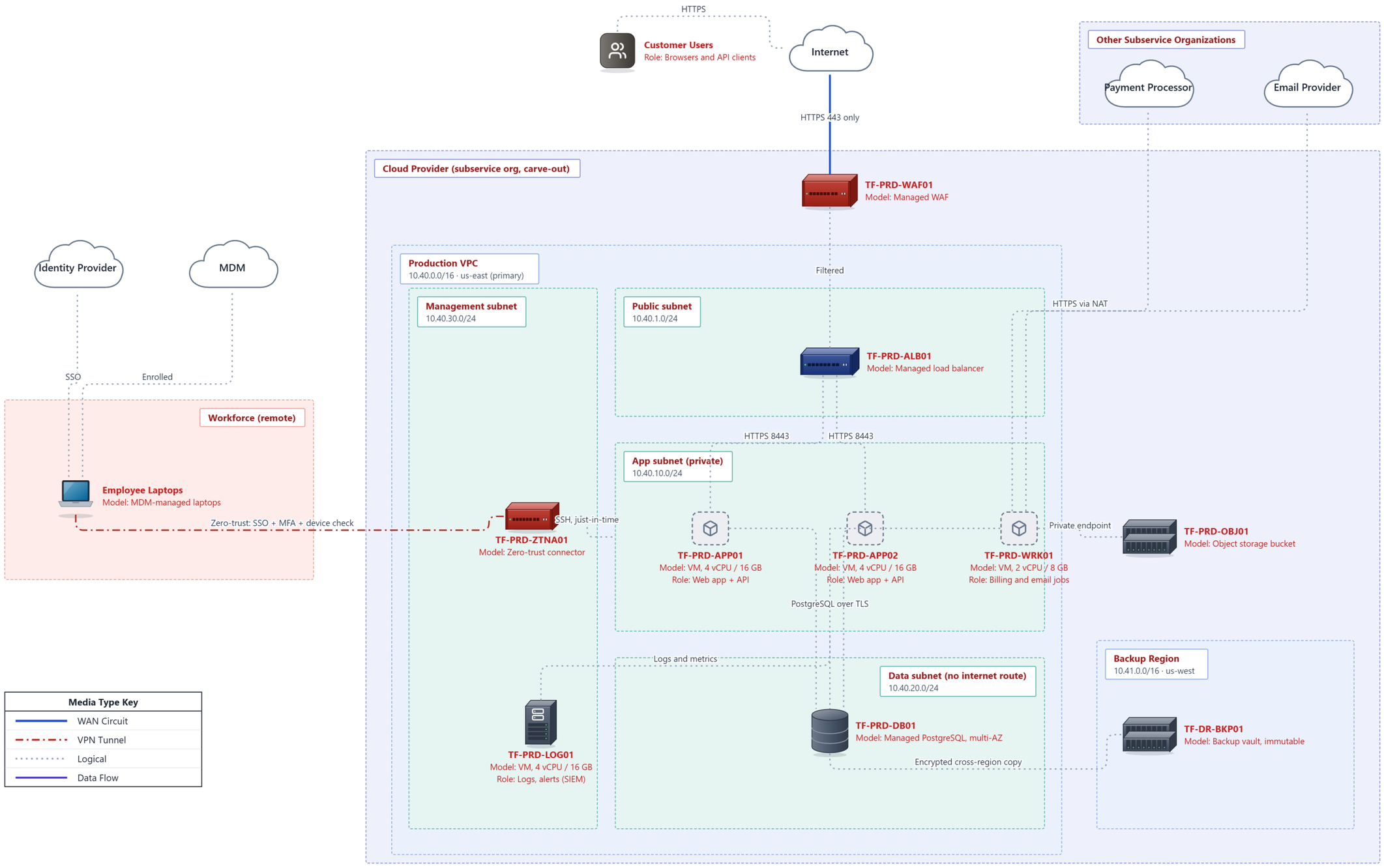
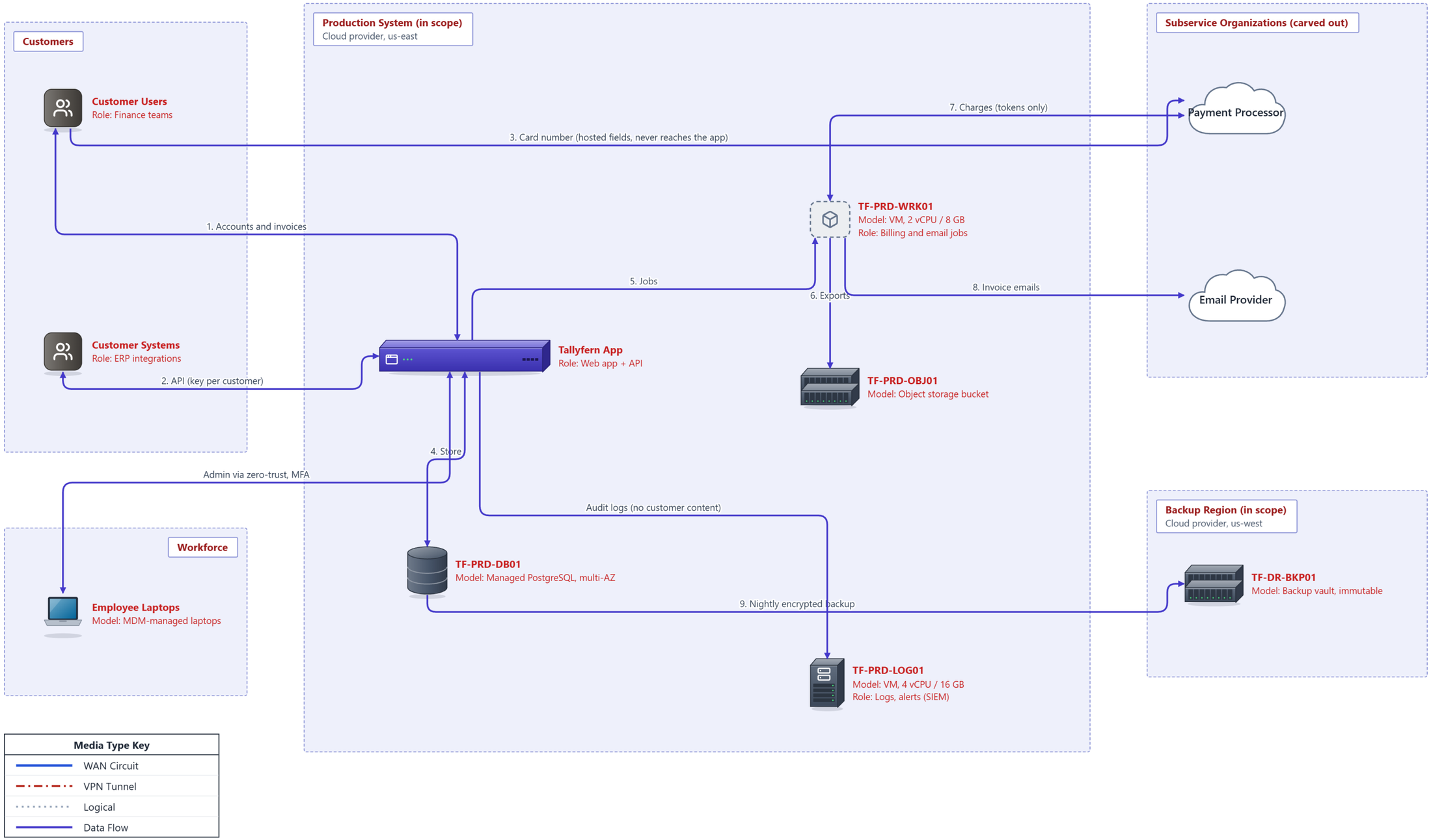


DOCUMENT **SOC 2 System Boundary - Production and Customer Data Flow** Tallyfern, Inc. · Remote-first; production in cloud provider us-east, backups in us-west	SHEET TITLE **Production System**	VERSION 1.0	LAST CHANGED 2026-11-25	VERIFIED
		DRAWN BY	LAST EDITOR	APPROVED



DOCUMENT
SOC 2 System Boundary - Production and Customer Data Flow
Tallyfern, Inc. · Remote-first; production in cloud provider us-east, backups in us-west

SHEET TITLE
Customer Data Flow

VERSION	LAST CHANGED	VERIFIED	SHEET
1.0	2026-11-25		2 of 7
DRAWN BY	LAST EDITOR	APPROVED	

Device Inventory 24 devices

Hostname	Type	Vendor / model	Serial	Mgmt IP	Area	Location	Page
Internet	Internet						Production System
TF-PRD-WAF01	Firewall	Cloud provider (IaaS) Managed WAF			Cloud Provider (subservice org, carve-out)		Production System
TF-PRD-ALB01	Load Balancer	Cloud provider (IaaS) Managed load balancer		10.40.1.10	Public subnet		Production System
TF-PRD-ZTNA01	VPN Gateway	Example Access Zero-trust connector		10.40.30.10	Management subnet		Production System
TF-PRD-LOG01	Server	Cloud provider (IaaS) VM, 4 vCPU / 16 GB		10.40.30.20	Management subnet		Production System
TF-PRD-APP01	Virtual Machine	Cloud provider (IaaS) VM, 4 vCPU / 16 GB		10.40.10.11	App subnet (private)		Production System
TF-PRD-APP02	Virtual Machine	Cloud provider (IaaS) VM, 4 vCPU / 16 GB		10.40.10.12	App subnet (private)		Production System
TF-PRD-WRK01	Virtual Machine	Cloud provider (IaaS) VM, 2 vCPU / 8 GB		10.40.10.21	App subnet (private)		Production System
TF-PRD-DB01	Database	Cloud provider (IaaS) Managed PostgreSQL, multi-AZ		10.40.20.10	Data subnet (no internet route)		Production System
TF-PRD-OBJ01	Storage / NAS	Cloud provider (IaaS) Object storage bucket			Cloud Provider (subservice org, carve-out)		Production System
TF-DR-BKP01	Storage / NAS	Cloud provider (IaaS) Backup vault, immutable			Backup Region		Production System
Payment Processor	Cloud Provider				Other Subservice Organizations		Production System
Email Provider	Cloud Provider				Other Subservice Organizations		Production System
Identity Provider	Cloud Provider						Production System
MDM	Cloud Provider						Production System
Employee Laptops	Laptop	Example Systems MDM-managed laptops			Workforce (remote)		Production System
Employee Laptops	Laptop	Example Systems MDM-managed laptops			Workforce		Customer Data Flow
TF-PRD-WRK01	Virtual Machine	Cloud provider (IaaS) VM, 2 vCPU / 8 GB		10.40.10.21	Production System (in scope)		Customer Data Flow
TF-PRD-OBJ01	Storage / NAS	Cloud provider (IaaS) Object storage bucket			Production System (in scope)		Customer Data Flow
TF-PRD-DB01	Database	Cloud provider (IaaS) Managed PostgreSQL, multi-AZ		10.40.20.10	Production System (in scope)		Customer Data Flow
TF-PRD-LOG01	Server	Cloud provider (IaaS) VM, 4 vCPU / 16 GB		10.40.30.20	Production System (in scope)		Customer Data Flow
Payment Processor	Cloud Provider				Subservice Organizations (carved out)		Customer Data Flow
Email Provider	Cloud Provider				Subservice Organizations (carved out)		Customer Data Flow
TF-DR-BKP01	Storage / NAS	Cloud provider (IaaS) Backup vault, immutable			Backup Region (in scope)		Customer Data Flow

Link / Cabling Schedule 17 links

Cable ID	End A	Interface	End B	Interface	Media	Speed	VLANs	Length	Test	Label / notes	Page
	Customer Users		Internet		Logical					HTTPS	Production System
	Internet		TF-PRD-WAF01		WAN Circuit					HTTPS 443 only	Production System
	TF-PRD-WAF01		TF-PRD-ALB01		Logical					Filtered	Production System
	TF-PRD-ALB01		TF-PRD-APP01		Logical					HTTPS 8443	Production System
	TF-PRD-ALB01		TF-PRD-APP02		Logical					HTTPS 8443	Production System
	TF-PRD-APP01		TF-PRD-DB01		Logical						Production System
	TF-PRD-APP02		TF-PRD-DB01		Logical					PostgreSQL over TLS	Production System
	TF-PRD-WRK01		TF-PRD-DB01		Logical						Production System
	TF-PRD-WRK01		TF-PRD-OBJ01		Logical					Private endpoint	Production System
	TF-PRD-WRK01		Payment Processor		Logical					HTTPS via NAT	Production System
	TF-PRD-WRK01		Email Provider		Logical						Production System
	TF-PRD-DB01		TF-DR-BKP01		Logical					Encrypted cross-region copy	Production System
	Employee Laptops		TF-PRD-ZTNA01		VPN Tunnel					Zero-trust: SSO + MFA + device check	Production System
	TF-PRD-ZTNA01		App subnet (private)		Logical					SSH, just-in-time	Production System
	TF-PRD-LOG01		App subnet (private)		Logical					Logs and metrics	Production System
	Employee Laptops		Identity Provider		Logical					SSO	Production System
	Employee Laptops		MDM		Logical					Enrolled	Production System

VLAN / Subnet Table 4 VLANs

VLAN	Name	Subnet	Gateway	DHCP scope / helper	Devices	Page
	App subnet (private)	10.40.10.0/24	10.40.10.1		3	Production System
	Data subnet (no internet route)	10.40.20.0/24	10.40.20.1		1	Production System
	Management subnet	10.40.30.0/24	10.40.30.1		2	Production System
	Public subnet	10.40.1.0/24	10.40.1.1		1	Production System

Data Flows 11 flows

From	To	Data	Class.	Sensitive data	Protocol / port	Encryption	Purpose	Page
Customer Users (Customers)	Tallyfern App (Production System (in scope))	Account, invoice and vendor details	Confidential	Personal info, Financial	HTTPS 443	TLS 1.3	Customers use the service	Customer Data Flow
Customer Systems (Customers)	Tallyfern App (Production System (in scope))	Invoices synced from ERP	Confidential	Financial	HTTPS 443 REST	TLS 1.2	Customer integrations	Customer Data Flow
Customer Users (Customers)	Payment Processor (Subservice Organizations (carved out))	Card number	Restricted	Card data	HTTPS 443	TLS 1.3	Customers pay their subscription; card data never reaches the app	Customer Data Flow
Tallyfern App (Production System (in scope))	TF-PRD-DB01 (Production System (in scope))	Accounts, invoices, payment tokens	Confidential	Personal info, Financial	PostgreSQL 5432	TLS 1.2	Store customer data	Customer Data Flow
Tallyfern App (Production System (in scope))	TF-PRD-WRK01 (Production System (in scope))	Billing and email jobs	Confidential	Personal info	Queue, HTTPS	TLS 1.2	Background processing	Customer Data Flow
TF-PRD-WRK01 (Production System (in scope))	TF-PRD-OBJ01 (Production System (in scope))	Uploads and CSV exports	Confidential	Personal info, Financial	HTTPS 443	TLS 1.2	Keep customer files	Customer Data Flow
TF-PRD-WRK01 (Production System (in scope))	Payment Processor (Subservice Organizations (carved out))	Payment token, amount	Internal		HTTPS 443	TLS 1.2	Charge subscriptions	Customer Data Flow
TF-PRD-WRK01 (Production System (in scope))	Email Provider (Subservice Organizations (carved out))	Name, email, invoice summary	Confidential	Personal info	HTTPS 443 API	TLS 1.2	Send invoices and notifications	Customer Data Flow
TF-PRD-DB01 (Production System (in scope))	TF-DR-BKP01 (Backup Region (in scope))	Encrypted snapshots	Confidential	Personal info, Financial	Provider snapshot copy	TLS 1.2	Backup and recovery (A1.2)	Customer Data Flow
Tallyfern App (Production System (in scope))	TF-PRD-LOG01 (Production System (in scope))	Audit and access logs	Internal		Syslog 6514	TLS 1.2	Monitoring (CC7.2)	Customer Data Flow
Employee Laptops (Workforce)	Tallyfern App (Production System (in scope))	Admin sessions	Confidential	Credentials	SSH 22 via ZTNA	SSH / SFTP	Support and administration, logged	Customer Data Flow

Data Stores 6 stores

Data store	Stores	Class.	Sensitive data	Encrypted at rest	Kept for	Region	Owner	Boundary
TF-PRD-DB01	Customer accounts, invoices, payment tokens	Confidential	Personal info, Financial	Yes	Contract term + 90 days	Primary region (us-east)	Engineering	Cloud Provider (subservice org, carve-out)
TF-PRD-OBJ01	Uploaded invoices and receipts, CSV exports	Confidential	Personal info, Financial	Yes	Contract term + 90 days	Primary region (us-east)	Engineering	Cloud Provider (subservice org, carve-out)
TF-DR-BKP01	Encrypted database snapshots and bucket replicas	Confidential	Personal info, Financial	Yes, customer-managed keys	35 days	Backup region (us-west)	Engineering	Cloud Provider (subservice org, carve-out)
TF-PRD-OBJ01	Uploaded invoices and receipts, CSV exports	Confidential	Personal info, Financial	Yes	Contract term + 90 days	Primary region (us-east)	Engineering	Production System (in scope)
TF-PRD-DB01	Customer accounts, invoices, payment tokens	Confidential	Personal info, Financial	Yes	Contract term + 90 days	Primary region (us-east)	Engineering	Production System (in scope)
TF-DR-BKP01	Encrypted database snapshots and bucket replicas	Confidential	Personal info, Financial	Yes, customer-managed keys	35 days	Backup region (us-west)	Engineering	Backup Region (in scope)