IntPowers

SECURITY AND COMPLIANCE DOSSIER

Transactional video for contact centers

Answers to the questions on a vendor risk questionnaire, in their order. Every control says who answers for it: us, the infrastructure, or your organization.



Since 2016
In production with banking and insurance customers

AWS
Infrastructure on dedicated nodes per customer

EU · US
Regions with storage assignment

SAML 2.0
Identity stays in your own directory

02 Scope and shared responsibility model

VENDOR AWS CUSTOMER

What this document covers and who answers for each layer. It is the first question in any assessment and it frames all the others.

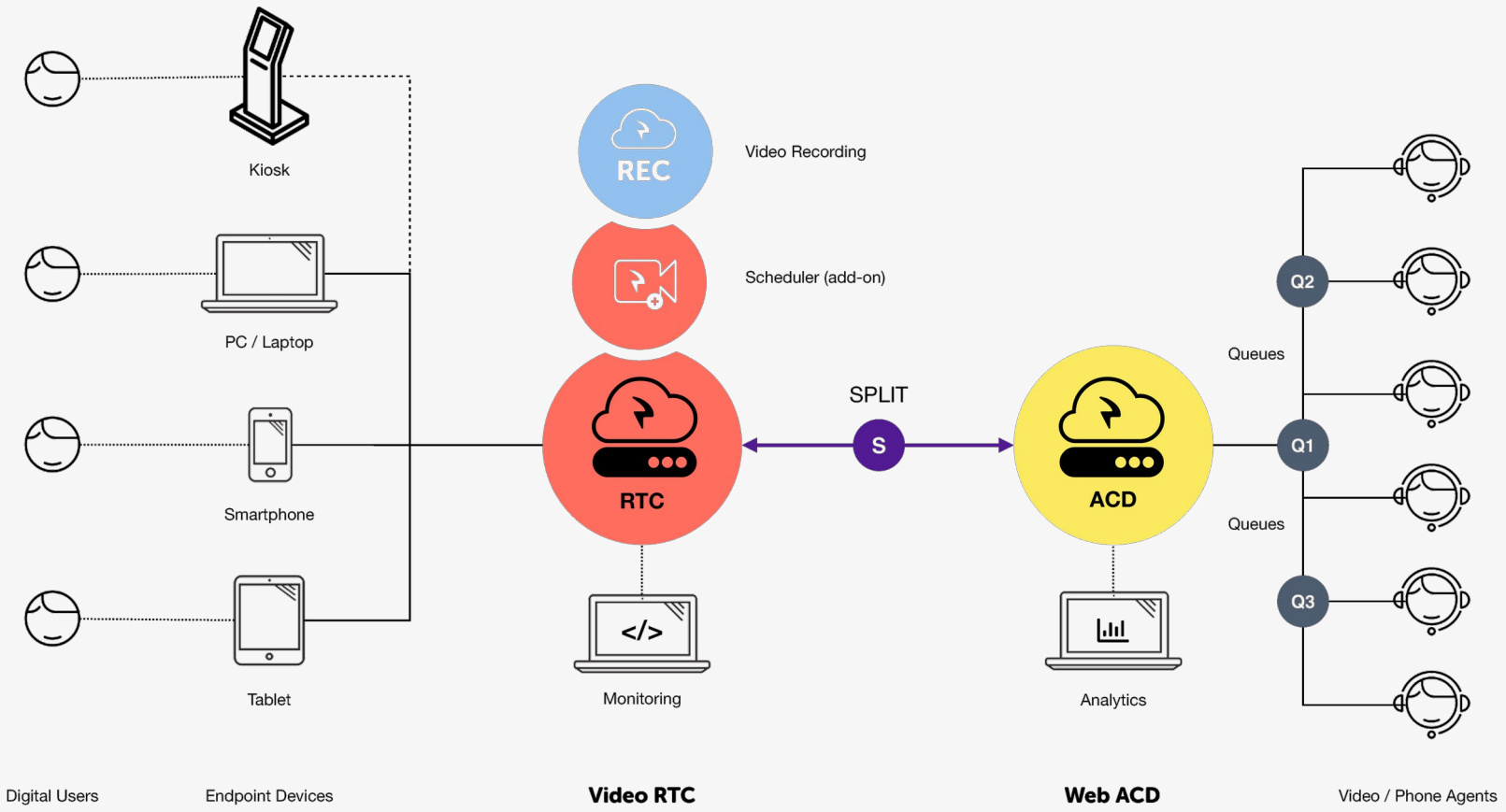
LAYER	WHO ANSWERS	WHAT IT INCLUDES
Physical and network infrastructure	**AWS**	Data centers, hypervisor, backbone network and its compliance program.
Platform and SPLIT gateway	**Vendor**	Dedicated nodes per customer, transcoding, STUN / TURN per region, recording storage.
Encryption of the WebRTC leg	**Vendor**	Always on, with 256-bit certificates and automatic renewal.
SRTP on the SIP trunk	**Customer**	Available when the trunk is connected; the customer switches it on per policy.
Identity and directory	**Customer**	The customer's Active Directory or SSO over SAML 2.0; the vendor integrates it.
Recording and retention policy	**Customer**	The customer decides what is recorded and for how long; the vendor executes it.
Monitoring and backups	**Vendor**	Proprietary ITSM monitoring and backups on AWS.
Agent desktop and internal network	**Customer**	The agent works from their usual tool; the customer network does not change.

IN ONE SENTENCE Only one leg of the session enters your network. Everything that happens on it is under your control.

03 Architecture and data flow

VENDOR AWS CUSTOMER

The components involved in a transactional video call and what each one carries. Recording and scheduling are separate pieces from the engine: they are switched on, not shipped on.



IN ONE SENTENCE The video engine, your distributor and your agents: three pieces, one SPLIT link between them.

04 Data inventory, residency and retention

VENDOR AWS CUSTOMER

Which data the service handles, where it resides, how it is protected and who decides how long it is kept.

DATA	WHERE IT RESIDES	PROTECTION	RETENTION
Real-time audio and video	Gateway, in the assigned region	Encrypted WebRTC	Not stored unless recording is on
SIP signaling and context	Your trunk and your platform	SRTP, if you enable it	Your platform's
RAW / MP4 recordings	REC storage, assigned region	AES 256 on export	Scheduled per service
Session metadata (SPLIT ID)	Your platform and REC	With the interaction	With the interaction
System logs	Nodes per region	No external access	Under NDA
REC access credentials	Your directory (SAML)	We do not hold them	Yours

IN ONE SENTENCE EU or US regional assignment by contract; dedicated keys, accounts and storage units when you require them.

05 Encryption and key management

VENDOR | AWS | CUSTOMER

What protects each leg and who switches it on. Real-time communications are encrypted with standard protocols, including peer-to-peer WebRTC connections and hybrid transcoding.

LEG	MECHANISM	WHO SWITCHES IT ON
Customer ↔ gateway	End-to-end encrypted WebRTC, with our own STUN / TURN per region, deployable on dedicated IPs.	Always on
Gateway ↔ your SIP trunk	SRTP over SIP, available when you connect your VoIP trunks.	You do
Certificates	Minimum length of 256 bits, private activation and automatic renewal.	Always on
Recording export	AES 256-bit on every record that leaves storage.	Always on
Network and administration	Firewalls, SSH, SSL / TLS and VPN across all systems.	Always on

DETAIL UNDER NON-DISCLOSURE AGREEMENT: Encryption at rest of recording storage · Key custody, rotation and use of KMS · Procedure for assigning dedicated keys per customer

IN ONE SENTENCE Two legs, two encryptions. The one that enters your network uses the one you already operate: SRTP.

06 Identity and access control

VENDOR AWS CUSTOMER

The recording environment is for corporate use, restricted to a limited number of users designated by security rules. It does not serve the agent tier.

Authentication

The customer's Active Directory over SAML 2.0, or external SSO (Google, Microsoft).

Accounts

Named per service, with password recovery by email.

Network restriction

IP-range filtering on top of directory authentication.

Per-service permissions

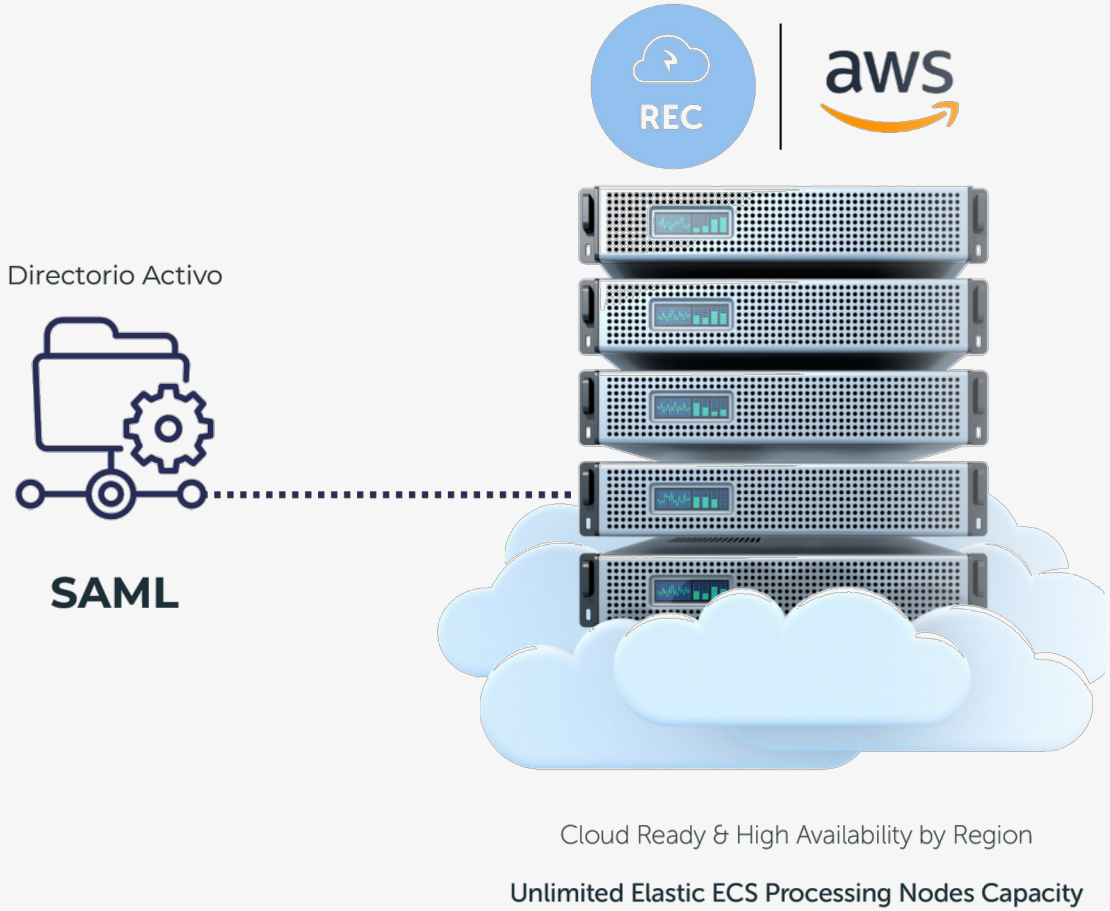
Auto-processing, HD, MP4 Player, Metadata, Flags and Deletion.

Deletion

Off by default; only at the customer's express request.

MFA on administrative accounts

Under NDA.



IN ONE SENTENCE The password never leaves your directory. We neither see it nor store it.

07 Segregation and isolation between customers

VENDOR AWS CUSTOMER

How one customer's data and processing are kept apart from another's, layer by layer.

LAYER	ISOLATION MECHANISM	SCOPE
Processing nodes	CPaaS on dedicated nodes that share no access between them.	Per customer
Storage	Dedicated storage units, enabled per service.	Per service
Keys and accounts	Specific activation options to assign dedicated keys and accounts.	Per customer
Network services	Our own STUN / TURN per region, deployable on dedicated IPs.	Per region or per customer
Region	Regional data assignment: EU, US and whichever the contract sets.	Per contract
Infrastructure	Physical and hypervisor isolation, under AWS's compliance program.	**AWS**

IN ONE SENTENCE Your data does not sit next to another customer's: not in processing, not in storage, not on the network.

08 Logging, audit and monitoring

VENDOR AWS CUSTOMER

There are two logging layers and it pays not to confuse them in an assessment: interaction traceability, which lives in your platform, and system logs, which live on our nodes.

WHAT IS LOGGED	WHERE	WHO ACCESSES IT	HOW IT IS DELIVERED
Events, recording and reporting for each video call	In your platform, as one more call	You, with your own tools	Already yours
Session metadata and input parameters	Through the unique SPLIT identifier	Your CRM, ERP or agent script	By integration
System logs: events, errors, warnings	Nodes per region; no service content	Only from inside the node	Specific traces, on request
Recording audit markers (Flags)	REC storage	Users holding the permission	In the dashboard
ITSM indicators per region, node and service	Our own monitoring on AWS	Our team; your IT where the contract provides	Shared dashboards

DETAIL UNDER NON-DISCLOSURE AGREEMENT: Retention period of system logs · Integration with the customer's SIEM

IN ONE SENTENCE Node logs are not exposed to external systems. Specific traces are enabled and delivered on request.

09 Recordings: the full lifecycle

VENDOR AWS CUSTOMER

Turning recording on is not directly operational, for security and privacy reasons: it is the customer's decision. From there, every step stays under their policy.

Activation

Set by your security policy. Recording type per plan: RAW; SD with MP4; HD.

Access

Named accounts with per-service permissions; preview and metadata per permission.

Retention

Storage periods scheduled per service.

Post-processing

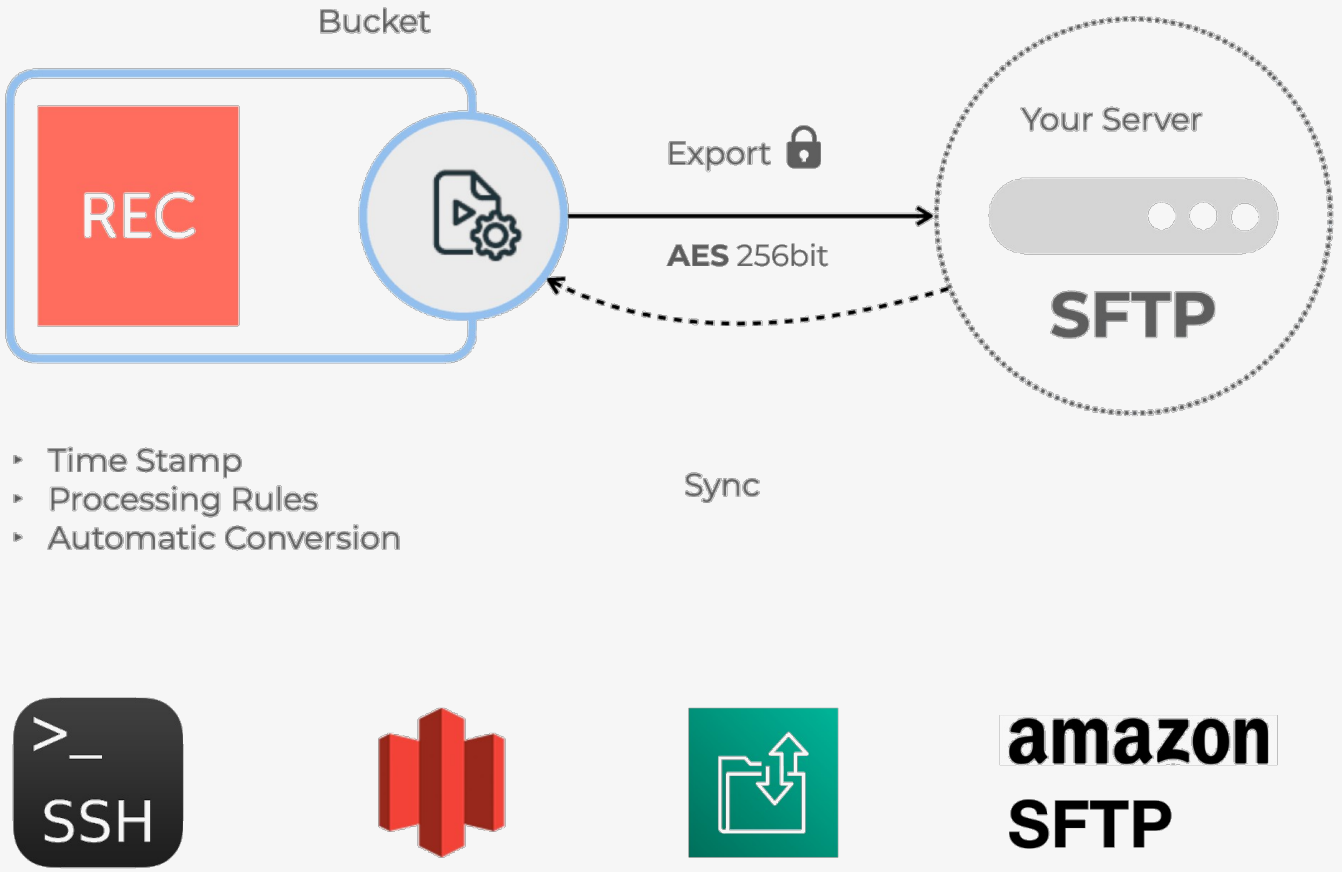
Instructions on receipt of each record: automatic deletion, SFTP export, archiving, backup.

Export

Programmable and automatic, encrypted with AES 256-bit, to your own server.

Deletion

Permission off by default; enabled only at express request.



IN ONE SENTENCE

This is the difference with a third-party video room: there the recording lives in another system, with another retention and another owner.

10 Vulnerability management and secure development

VENDOR AWS CUSTOMER

The criteria the platform is developed and operated under, and the process that sustains them.

PRINCIPLE	WHAT IT MEANS IN PRACTICE
Application security	Preventing unauthorized access, use, disclosure, disruption, modification or destruction of the application and its data.
Network security	Firewalls, SSH, SSL, TLS and VPN, with controls that evolve with specific knowledge.
Proven product security	All access with 256-bit certificates to encrypt communications and protocols.
Data center management	Automation, monitoring and management on AWS.
The data belongs to the customer	Dedicated nodes with no shared access between services.

DETAIL UNDER NON-DISCLOSURE AGREEMENT:

Patching cadence for systems and dependencies · External penetration testing: frequency and latest report · Responsible disclosure program · Code review and change management

IN ONE SENTENCE

The principles are written down. The process that audits them is delivered with the dossier.

11 Continuity and recovery

VENDOR AWS CUSTOMER

A documented Disaster Recovery Plan and a security document system exist. These are its recovery figures per region.

Data backup · EU

Minimum 1 day · standard 7 days · maximum 14 days.
AWS Backup.

Directory sync · EU

Minimum 1 month · standard 2 months · maximum 1 year.
Directory Sync.

Data backup · US

Minimum 1 day · standard 7 days · maximum 14 days.
AWS Backup.

Directory sync · US

Minimum 1 month · standard 2 months · maximum 1 year.
Directory Sync.



DETAIL UNDER NON-DISCLOSURE AGREEMENT:

RTO per severity level · Restoration procedure and owners per service

IN ONE SENTENCE Critical servers and services connected to backups spanning weeks or months, with per-region restoration.

12 Incident response

VENDOR AWS CUSTOMER

What this document already covers for each phase, and what is delivered under NDA: the full incident response procedure.

PHASE	WHAT IS ALREADY IN THIS DOCUMENT	SECTION
Detection	Own ITSM monitoring system per region, node and service, with dashboards shared with your team.	8
Traceability	System logs on per-region nodes, not reachable from outside; specific traces delivered on request.	8
Containment	Processing nodes, storage and keys dedicated per customer, with no shared access between services.	7
Recovery	AWS Backup copies and directory sync per region, with per-service restoration.	11

DETAIL UNDER NON-DISCLOSURE AGREEMENT

- Incident classification and severity levels
- Notification deadline to the customer and to the supervisory authority
- Escalation chain and owners
- Communication during the incident and post-incident analysis
- Coordination with the customer's security team

It exists and is delivered with the full dossier. Ask for it before due diligence, not during.

IN ONE SENTENCE A bank does not ask whether you have a procedure. It asks how many hours until you call.

13 Sub-processors and third parties

VENDOR AWS CUSTOMER

Who else takes part in delivering the service, and with what scope.

FUNCTION	WHO PROVIDES IT	WHERE AND HOW	REGION
Compute, network and storage	**AWS**	Nodes and storage units dedicated per customer, within the AWS compliance program.	EU · US, per contract
Backups	**AWS**	AWS Backup, with 1, 7 and 14-day retention.	Per region
SPLIT gateway and transcoding	**Vendor**	Own nodes. Not subcontracted.	Per region
STUN / TURN	**Vendor**	Own servers with dedicated IPs, deployable per customer.	Per region
Identity	**Customer**	Your Active Directory or SSO. We do not hold credentials.	Yours
SIP connectivity	**Customer**	Your trunk and your carrier; SRTP available once connected.	Yours

DETAIL UNDER NON-DISCLOSURE AGREEMENT:

Full list of sub-processors and their processing agreements · SIP connectivity and network providers, where applicable · Procedure for notifying changes to the list

IN ONE SENTENCE

We are an AWS Standard Technology Partner. The infrastructure is not subcontracted to anyone else.

14 Certifications and attestations

VENDOR AWS CUSTOMER

An infrastructure certificate is not a vendor certificate. We keep them apart so nobody has to work it out halfway through an assessment.

What Interactive Powers attests

On its Video RTC listing on Genesys AppFoundry

GDPR

HIPAA

If your procurement requires an attestation that is not in this column, say so in the first meeting: that is a conversation about timing.

What the infrastructure certifies

Amazon Web Services compliance program, where we run. The seals on the right, ISO 27001 included, belong to AWS, not to Interactive Powers.

Verifiable at aws.amazon.com/compliance. Interactive Powers is an AWS Standard Technology Partner.



SOC 1



SOC 2



SOC 3



ISAE 3402



PCI



MPAA



FISMA



ISO27001



HIPAA

IN ONE SENTENCE Neither SOC 2 nor ISO 27001 is attested today by Interactive Powers: they are AWS's. We say so here so it need not be explained later.

15 Documentation available under NDA

VENDOR | AWS | CUSTOMER

What exists in writing and is delivered under a non-disclosure agreement. Ask for it before due diligence, not during.

Disaster Recovery Plan

Recovery objectives, RTO per severity, owners and procedure per service. Section 11.

Security document system

Internal security procedures and their version control. Section 10.

Key management

Custody, rotation, KMS and dedicated key assignment. Section 5.

Vulnerability management

Patching cadence, pentest reports, responsible disclosure. Section 10.

Incident response

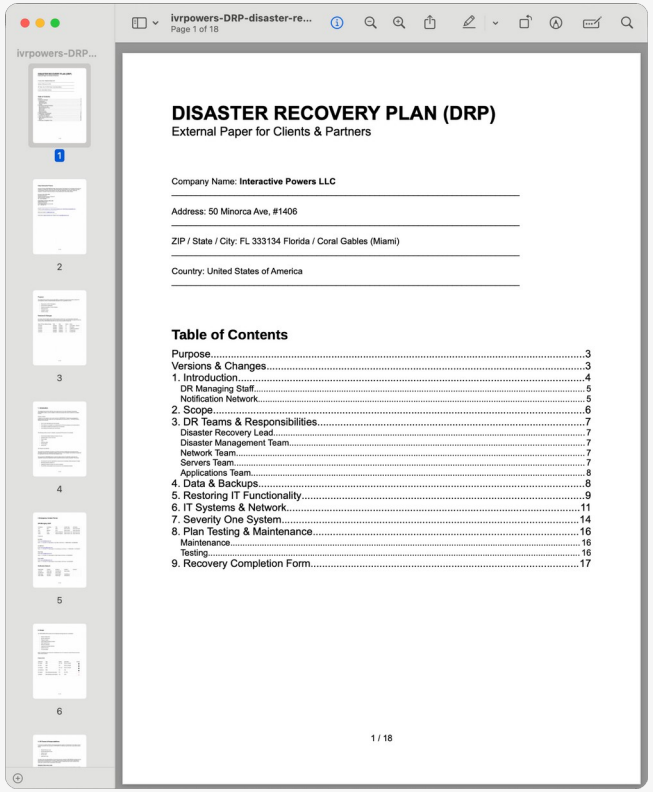
Classification, notification deadlines, escalation and communication. Section 12.

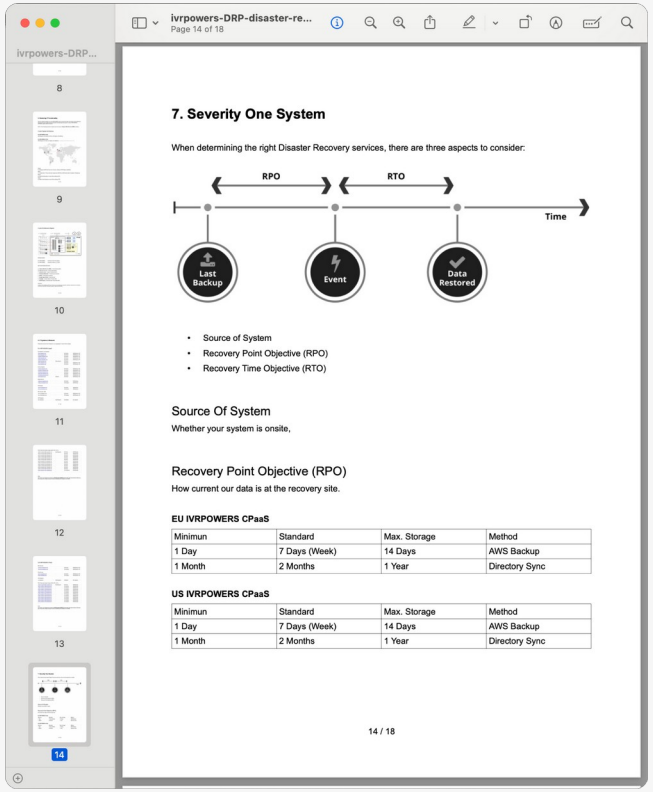
Sub-processors

Full list and processing agreements. Section 13.

Log retention and SIEM

Retention periods and integration options. Section 8.





IN ONE SENTENCE Put your security team in the first meeting, not the last.

IntPowers

The security conversation is better had at the start.

Whatever is unresolved, we say so in the first meeting, not the last.



Talk to Engineering

Request the dossier

Under NDA
Seven documents, listed in section 15

Madrid · Miami
Support in CET and EST hours

interactivepowers.com
Public platform documentation

AWS Partner
Standard Technology Partner

Interactive Powers, SL (Europa) o LLC (America) operan como IntPowers o IVRPowers