IntPowers × GENESYS

SECURITY DOSSIER · GENESYS CLOUD

Transactional video in Genesys Cloud

Answers to a vendor risk questionnaire for Genesys Cloud accounts. Each control states who is responsible: us, the infrastructure or your organization.



Since 2019

Genesys AppFoundry Premium Partner

AWS

Infrastructure on dedicated nodes per customer

EU · US

Regions with storage assignment

Genesys login

Agents sign in with their Genesys Cloud account

02 Scope and shared responsibility model

VENDOR AWS CUSTOMER

What this document covers and who is responsible for each layer. Your Genesys Cloud platform is part of your organization: it appears as “Customer”.

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 and the SIP link to your Genesys Cloud.
Encryption of the WebRTC leg	**Vendor**	Always on, with 256-bit certificates and automatic renewal.
SPLIT trunking	**Vendor**	SIP link between the gateway and your Genesys Cloud; SRTP per your policy.
Agent identity	**Customer**	Agents sign in with their Genesys Cloud account; the SPLIT widgets use that session.
Recording and retention policy	**Customer**	Genesys records the voice per your policy; video only if you enable Video REC.
Monitoring and backups	**Vendor**	Proprietary ITSM monitoring and backups on AWS.
Agent desktop and network	**Customer**	Agents work in Genesys Cloud with the SPLIT widgets; network per CCaaS requirements.

IN ONE SENTENCE Voice enters Genesys as one more call. Video travels through our gateway, encrypted.

03 Genesys Cloud integration

VENDOR AWS CUSTOMER

How Video RTC integrates into your Genesys Cloud organization and who is responsible for each touchpoint with the platform.

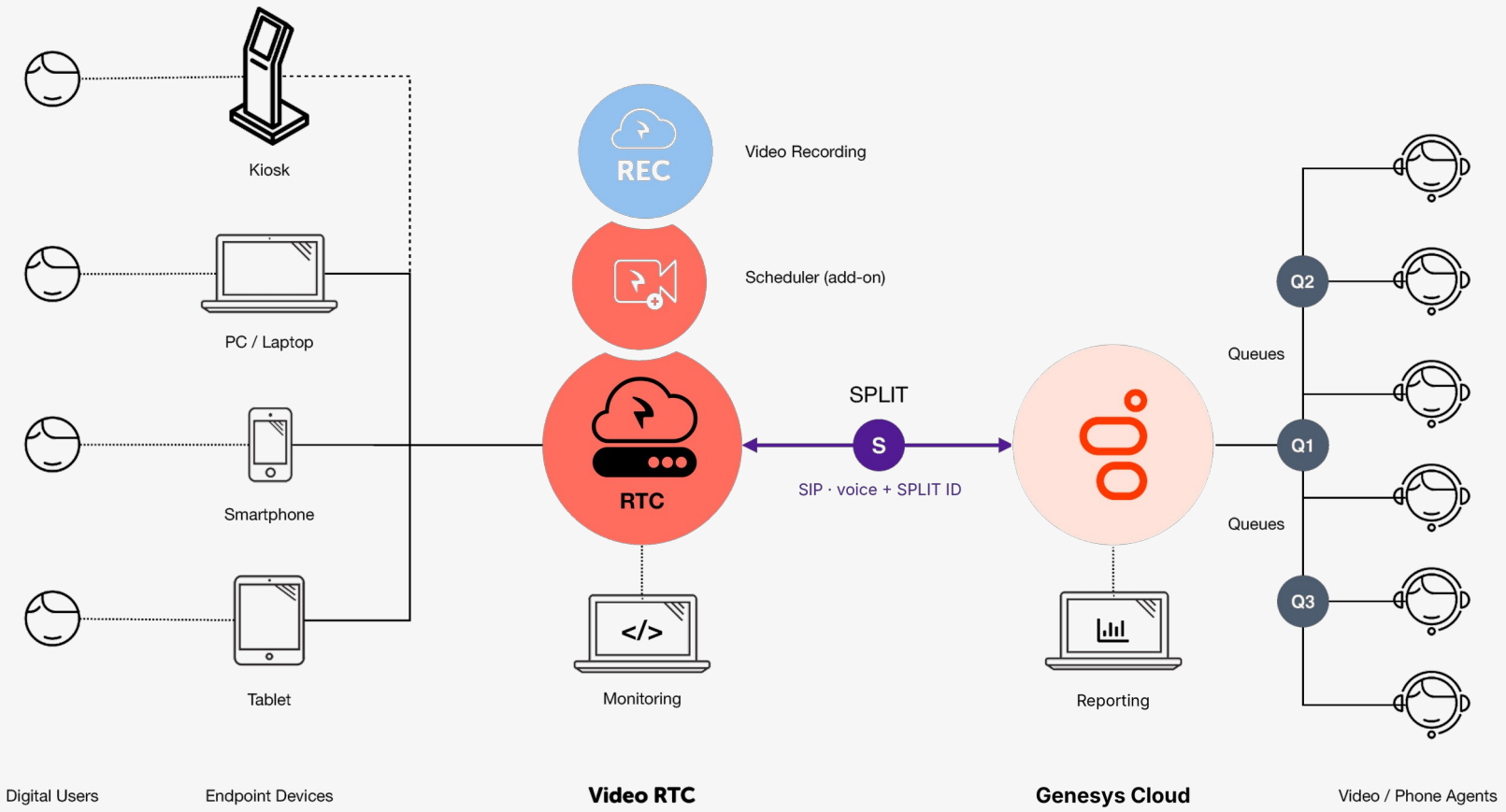
INTEGRATION POINT	WHO ANSWERS	WHAT IT MEANS
Genesys AppFoundry listing	**Vendor**	Video RTC for Genesys, Premium Partner since 2019; contracted with Interactive Powers.
SPLIT trunking	**Vendor**	The video call enters your Genesys Cloud organization as one more call, over SPLIT trunking: the SIP connection we use to link any CCaaS.
Routing	**Customer**	Genesys Architect, queues, skills and priorities: the call never leaves your flow.
Agent control	**Customer**	Answer, hold, transfer and consult from the interaction bar and the dialpad.
SPLIT widgets	**Vendor**	Video Session, Scheduled, Reverse, Messaging and Remote Viewer, inside Genesys.
Agent video	**Vendor**	SPLIT Agent window and PiP; video arrives encrypted over WebRTC from the gateway.
Recording	**Customer**	Voice in Genesys recording; video in Video REC only if you enable it.
Context and reporting	**Customer**	Widget data in SIP headers for Architect; the video call counts in your KPIs.

IN ONE SENTENCE The interaction lives in your Genesys Cloud; we provide the video and its gateway.

04 Architecture and data flow

VENDOR AWS CUSTOMER

The components of a transactional video call in Genesys Cloud and where each one passes. Video recording is a separate piece: it is enabled, not on by default.



IN ONE SENTENCE Genesys routes the voice; our gateway carries the video. One SPLIT identifier links them.

05 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
Video call voice	Your Genesys Cloud, with its recording	SRTP, if you enable it	Your Genesys policy
Video recordings	Video REC, assigned region	AES 256 on export	Scheduled per service
SPLIT ID and parameters	Your Genesys and the gateway	Only those of the session	No copy of Genesys data
System logs	Nodes per region	No external access	Under NDA
Agent credentials	Your Genesys Cloud organization	We do not hold them	Yours

IN ONE SENTENCE EU or US regional allocation by contract. Voice and its recording stay in your Genesys Cloud.

06 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 and 256-bit certificates.	Always on
Gateway ↔ Genesys Cloud	Voice leg over SPLIT trunking (SIP); SRTP available per your policy.	You do
Gateway ↔ agent widget	Encrypted WebRTC video to the agent's browser, inside Genesys Cloud.	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 Three legs. The one entering Genesys runs over SPLIT trunking, with SRTP if you enable it.

07 Identity and access control

VENDOR AWS CUSTOMER

Agents have no account with us: they sign in to Genesys Cloud and the SPLIT widgets use that session. The video recording environment is separate and for corporate use.

Agent authentication

Their Genesys Cloud account; the SPLIT widgets use that session.

Agent permissions

Roles and queues of your Genesys organization; we create no agent accounts.

Network restriction

IP-range filtering on top of directory authentication.

Video REC access

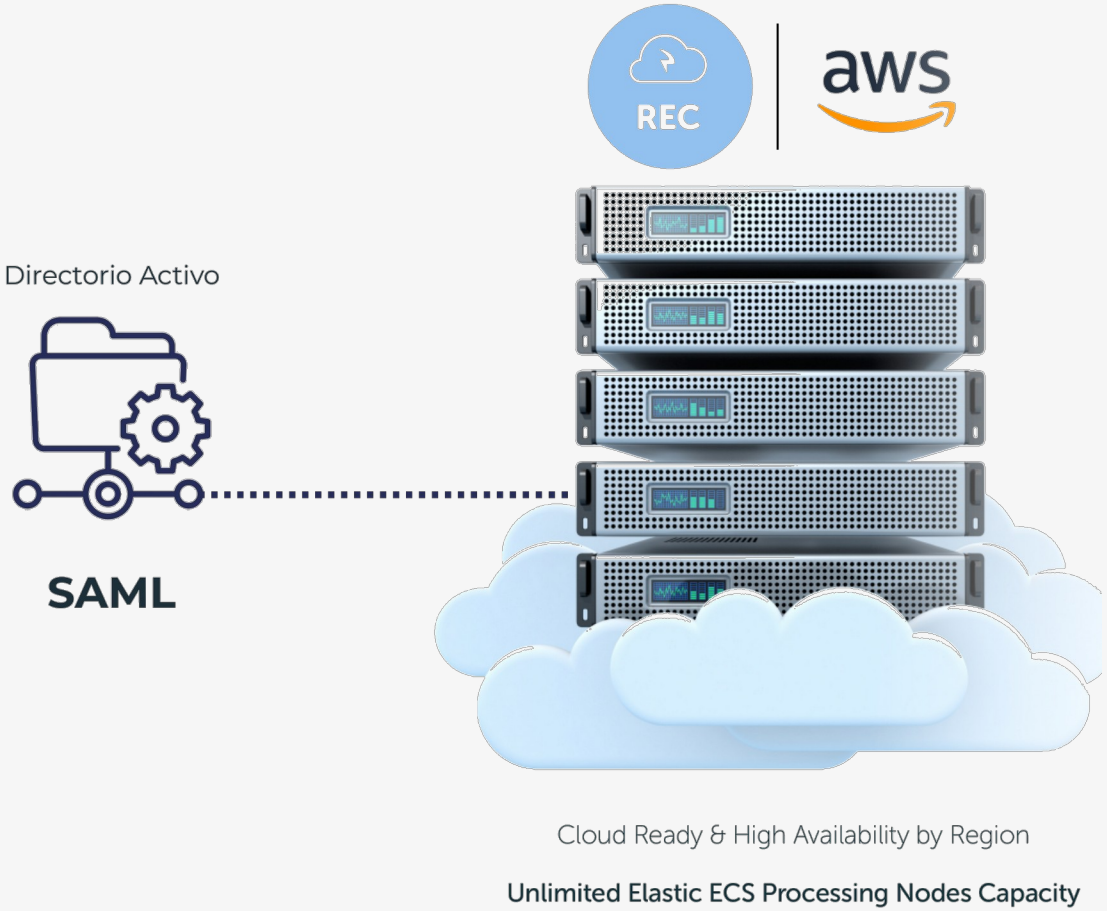
Active Directory via SAML 2.0 or external SSO; named accounts.

Deletion

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

MFA on administrative accounts

Under NDA.



IN ONE SENTENCE The agent's password never leaves Genesys. We neither see it nor store it.

08 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.

09 Logging, audit and monitoring

VENDOR AWS CUSTOMER

There are two logging layers and they should not be confused: interaction traceability, which lives in Genesys Cloud, and system logs, which live on our nodes.

WHAT IS LOGGED	WHERE	WHO ACCESSES IT	HOW IT IS DELIVERED
Events, voice recording and reporting	In Genesys Cloud, as one more call	You, with Genesys tools	Already yours
Session metadata and input parameters	Through the unique SPLIT identifier	Your Genesys, CRM 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.

10 Recordings: the full lifecycle

VENDOR AWS CUSTOMER

Genesys records the voice under its policy. Video is recorded only if you enable Video REC, and from there every step follows your 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

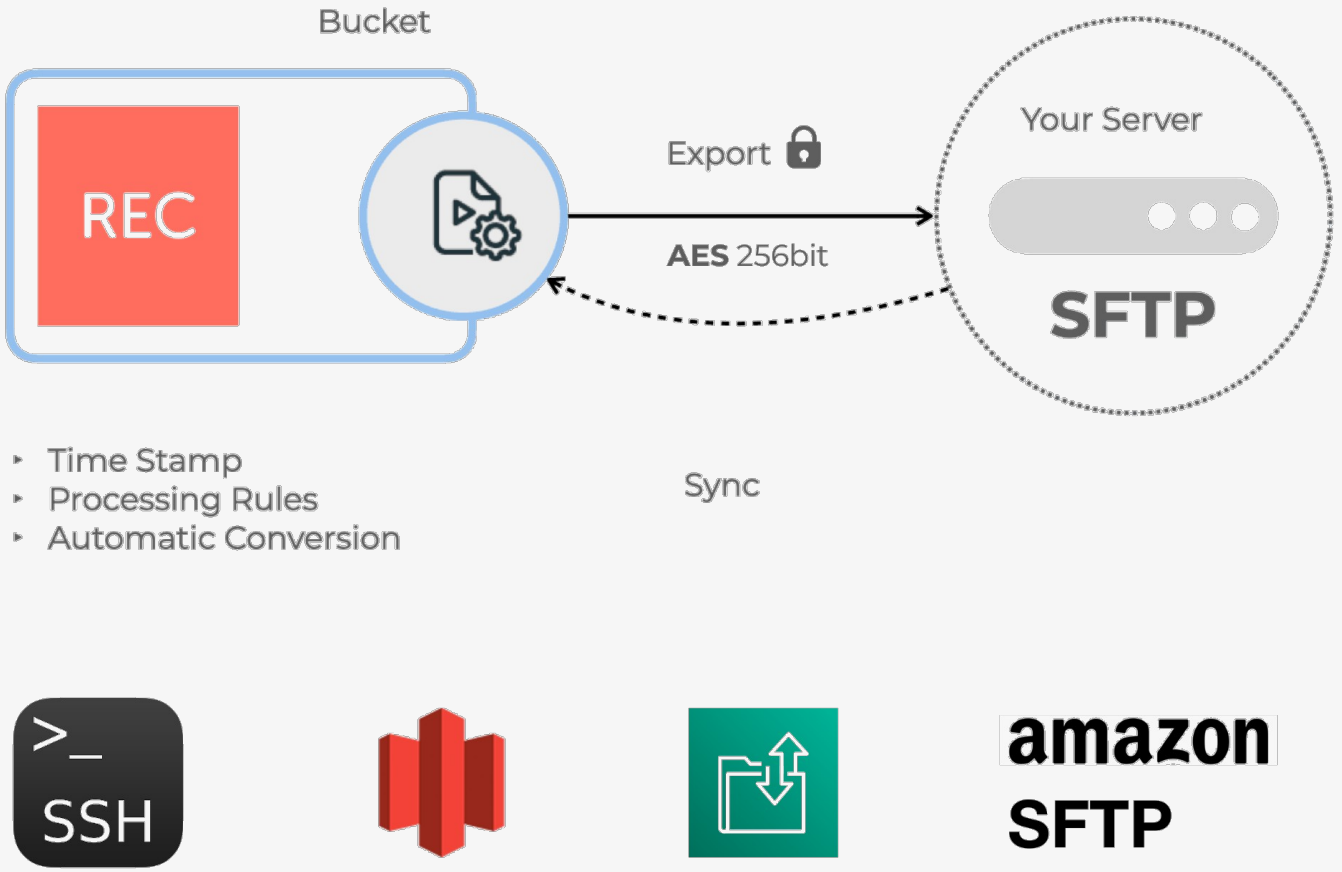
Instructions on receipt of each record: automatic deletion, SFTP export, archiving, backup.

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

Voice in Genesys and video in Video REC: both recordings under your policy, with the same SPLIT identifier.

11 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.

12 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.

13 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.	9
Traceability	System logs on per-region nodes, not reachable from outside; specific traces delivered on request.	9
Containment	Processing nodes, storage and keys dedicated per customer, with no shared access between services.	8
Recovery	AWS Backup copies and directory sync per region, with per-service restoration.	12

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.

14 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
Agent identity	**Customer**	Your Genesys Cloud organization. We hold no credentials.	Yours
Voice and voice recording	**Customer**	Your Genesys Cloud, connected over SPLIT trunking; SRTP available.	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.

15 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.

16 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 12.

Security document system

Internal security procedures and their version control. Section 11.

Key management

Custody, rotation, KMS and dedicated key assignment. Section 6.

Vulnerability management

Patching cadence, pentest reports, responsible disclosure. Section 11.

Incident response

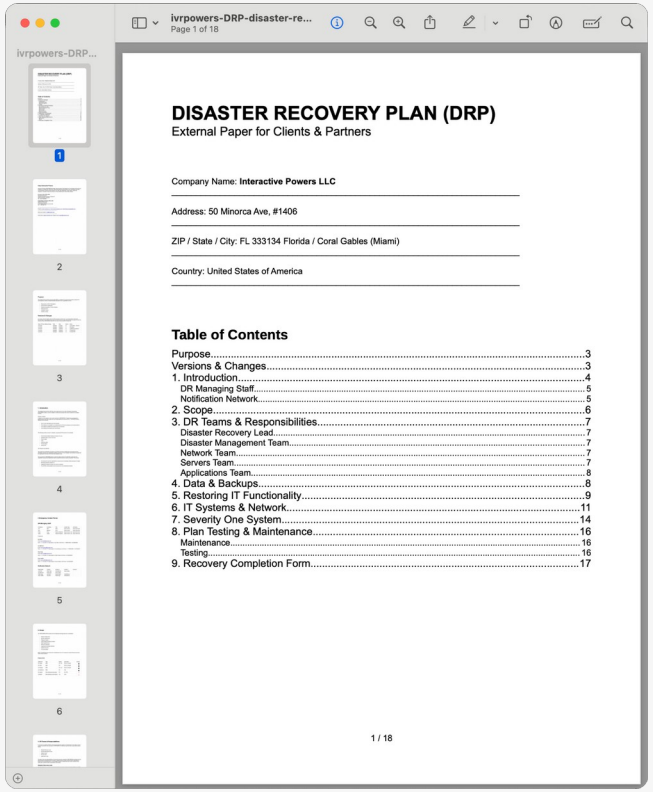
Classification, notification deadlines, escalation and communication. Section 13.

Sub-processors

Full list and processing agreements. Section 14.

Log retention and SIEM

Retention periods and integration options. Section 9.



DISASTER RECOVERY PLAN (DRP)
External Paper for Clients & Partners

Company Name: **Interactive Powers LLC**

Address: 50 Minorca Ave, #1406

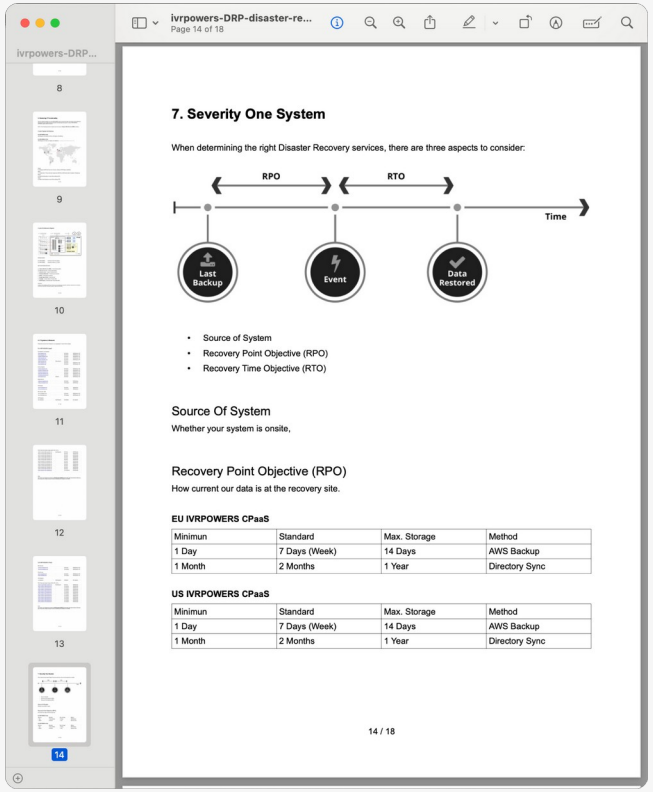
ZIP / State / City: FL 333134 Florida / Coral Gables (Miami)

Country: United States of America

Table of Contents

Purpose....3
Versions & Changes....3
1. Introduction....4
DR Managing Staff....5
Notification Network....5
2. Scope....6
3. DR Teams & Responsibilities....7
Disaster Recovery Lead....7
Disaster Management Team....7
Network Team....7
Servers Team....7
Applications Team....8
4. Data & Backups....8
5. Restoring IT Functionality....9
6. IT Systems & Network....11
7. Severity One System....14
8. Plan Testing & Maintenance....16
Maintenance....16
Testing....16
9. Recovery Completion Form....17

1 / 18



7. Severity One System

When determining the right Disaster Recovery services, there are three aspects to consider:

- Source of System
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

Source Of System

Whether your system is onsite,

Recovery Point Objective (RPO)

How current our data is at the recovery site.

EU IVRPOWERS CPaaS

Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

US IVRPOWERS CPaaS

Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

14 / 18

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

IntPowers × GENESYS

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 16

Madrid · Miami
Support in CET and EST hours

AppFoundry
Genesys Premium Partner since 2019

AWS Partner
Standard Technology Partner

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