
TC ENTERTAINMENT (TCE)

BETTING

DISASTER & RECOVERY PLAN

TC ENTERTAINMENT

TC ENTERTAINMENT

1 Notations

1.1 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents (“the documents”) are the property of TC Entertainment N.V. (TENV). Unauthorised copying and distribution of the documents, by any means, on any media is prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The documents are copyright.

1.2 Version

Version	Description	By	Date
1.4	Updates		

1.3 Copyright Notice

© Copyright Notice

1. All copyright and other intellectual property rights subsisting in TC Entertainment N.V., functional and technical documentation is owned or licensed by TC Entertainment N.V. and protected by the laws of Curacao and other countries.
2. Persons must not otherwise reproduce, transmit (including broadcast), communicate, adapt, distribute, sell, modify or publish or otherwise use any of the documentation, except with the prior written consent of TC Entertainment N.V.

2 Administration

2.1 Table of contents

1	Notations	2
1.1	Confidentiality	2
1.2	Version	2
1.3	Copyright Notice	2
2	Administration	3
2.1	Table of contents	3
3	Introduction	4
3.1	Background	4
3.2	Purpose of disaster / recover plan.....	4
3.3	Structure of disaster / recover plan.....	4
3.4	Disaster / recovery plan implementation phase.....	4
4	Network And Applications	5
4.1.1	Production network (Netherlands)	5
4.1.2	Disaster / recovery network (Netherlands)	5
4.2	TENV Applications	7
4.2.1	TENV Betting Website.....	7
4.2.2	Email system / live chat.....	7
4.2.3	Security incident / problem reporting	7
4.2.4	Third-party systems	8
4.2.5	Financial system	8
4.2.6	Software Development System	8
5	TENV data backups / restore / test restore	10
5.1	Customer data.....	10
5.2	Event / pricing data.....	11
5.3	Corporate data	11
5.4	Other data	11
5.4.1	Source code	11
5.4.2	Documentation	11
5.4.3	Logs	11
5.4.4	Configuration files	11
5.4.5	Local GITLAB Tickets	11
5.4.6	Voice recordings	11
6	Disaster recovery personnel	12
6.1	Disaster Response Management Team	12
6.2	TENV Departments.....	12
6.3	Contact List	13
7	Disaster / recovery situation assessment	0
8	Disaster / recovery / resumption procedures	1
8.1	Production network disaster situation.....	1
8.1.1	Production network – level 1 disaster	1
8.1.2	Production network – level 2 disaster	1
9	Test disaster / recovery plan	2
9.1	Test production network disaster recovery plan.....	2
9.2	Test head office network disaster recovery plan	2
10	End of document	2

3 Introduction

3.1 Background

Disaster Recovery is the process, policies and procedures of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (incoming, outgoing, toll-free, fax, etc.), workspace, and other business processes after a [natural](#) or [human-induced disaster](#).

3.2 Purpose of disaster / recover plan

To increase the opportunity for a successful recovery to normal business operations, a well-established and thoroughly tested data recovery plan has been developed.

The disaster recovery plan (DRP) includes plans for coping with the unexpected or sudden loss of communications and/or key personnel.

The Disaster Recovery Plan seeks to ensure TENV's Business Continuity by providing contingency plans that address the potential loss of critical information resources (e.g., computers, terminals, and telecommunications equipment).

The purpose of the TENV Disaster Recovery Plan is to enable TENV totally resume normal operations on the critical business applications approximately one hour after the decision has been made to failover to the Disaster Recovery Hot Site.

3.3 Structure of disaster / recover plan

The TENV Disaster / Recovery Plans include the following sections:

- Section 4 – TENV Assets;
- Section 5 – TENV Backups / Restore / Test Restore;
- Section 6 – Identified Threats and Risks;
- Section 7 – Disaster / Recovery Personnel;
- Section 8 – Disaster / Recovery Communications;
- Section 9 – Disaster / Recovery Situation Assessment;
- Section 10 – Disaster / Recovery / Resumption Procedures;
- Section 11 – Test Disaster / Recovery Plan '

Procedures are detailed describing to changeover from the production site to the D/R hot site.

This includes such things as: notification procedures, phone change over procedures, phone recorder changeover procedures, trading floor workstations, internet connectivity changeover procedures, DNS changeover procedures, applications changeover procedures, database changeover procedures, and finally return to primary site procedures;

3.4 Disaster / recovery plan implementation phase

- **Phase –Production Network Disaster Recovery Site**

This phase would establish a production site in one data centre in Netherlands and disaster /recovery **network in a different data centre** (mentioned in 3.4.2) in Netherlands. If the production network becomes inoperative, operations on the production network will be suspended and will transfer to the disaster / recover site.

4 Network And Applications

4.1.1 Production network (Netherlands)

The TENV production network is located at LeaseWeb (Netherlands) - J.W. Lucasweg 35, 2031 BE Haarlem, The Netherlands. All equipment associated with TENV are located in an approved hosting site and housed in secure racks.

To protect and isolate the customer database from security breaches from the outside world, the network design has incorporated a perimeter and internal network structure. There are external and internal firewalls to protect the external and internal networks.

The TENV production network perimeter network includes:

- Routers
- Switches
- Firewalls
- Intrusion Protection Servers

The TENV production network internal network includes:

- Web Servers
- Database Server
- Data Storage

In addition, the network design has also incorporated the use of VLAN's to segregate the DMZ (demilitarized zones) and the various servers and services in the network.

The DMZ's on the TENV production network include:

- VLAN2 – Web Servers
- VLAN3 – Customer Database / Data Storage
- VLAN4 - Firewall Management

Customer data is replicated real-time to the TENV disaster / recovery network and to the TENV Disaster site in Netherlands.

4.1.2 Disaster / recovery network (Netherlands)

The TENV disaster / recovery network is located at Leaseweb (Netherlands) – Luttenbergweg 8, 1101 EC Amsterdam-Zuidoost, Netherlands. All equipment associated with TENV is located in an approved hosting site and housed in secure racks.

Web Sites:

Web Sites:

-Single page application Angular frontend website (www.hititbet.com), **192.168.3.21 (External I.P : 85.17.210.33)**. Mobile site is m.hititbet.com on the same IP.

-Single page application Angular frontend website (www.betorder.com), **192.168.3.21 (External I.P : 85.17.210.33)**. Mobile site is m.betorder.com on the same IP.

--Single page application Angular frontend website (www.bets4you.com), **192.168.3.202 (External I.P : 85.17.210.44)**. Mobile site is m.bets4you.com on the same IP.

-Single page application Angular frontend website (www.globalbahis.com), **192.168.3.202 (External I.P : 85.17.210.44)**. Mobile site is m.globalbahis.com on the same IP.

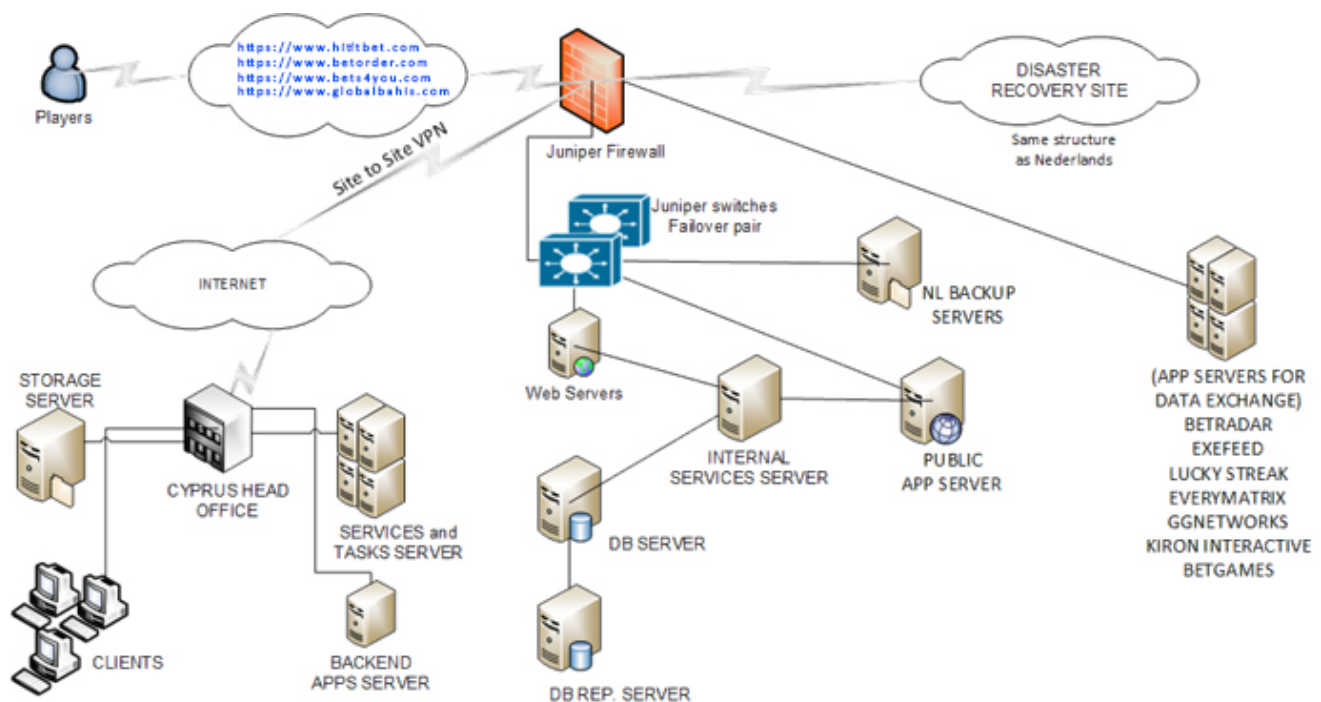
- All operations are carried of in a secure backend api

- All background services and tasks run in a separeate server with internal ip

-All public websites (desktop, mobile or postback) are secured with SSL.

-Note that all external traffic is managed and forwarded using NAT Rules therefore all the external I.P will be the same on the user end.

Architecture Overview Diagram :



4.2 TENV Applications

4.2.1 TENV Betting Website

Customer facing applications include:

Customer Registration / Login – In this function, customers can register their account by entering all the necessary personal information required to start a Poker session on the website. In addition, there is marketing information that is requested from the customer – it is optional; Once they are successfully registered they can login into the TENV website;

Customer Betting Session – This application can be defined as the most critical application in the system as it is the revenue generating vehicle for the organization. This application provides a variety of ways for customers to wager on Poker.

Customer Payment Processor Registration – Once the customer has registered and they wish to wager on TENV website, they must register a credit card, debit card , bank account or **integrated third party certified payment processors or online wallets** so they can deposit funds into their account;

Customer Deposits – Once the payment method has been determined and registered, the customer can deposit an initial amount of up to **5000 Euros. However, before the customer can deposit more funds, they must supply valid ID;**

Customer Withdrawals – Once the payment method has been determined and registered, the customer can withdraw an the amount in their account there is no withdraw limit. **However, before the customer can withdraw funds, they must supply valid ID;**

If the Betting website is not operational customers are unable to access their accounts or wager - this is a level 1 disaster situation;

4.2.2 Email system / live chat

In support of the TENV , the Email system is used by Customer Service to communicate to customers. It is also used by the rest of the organization to communicate internally and externally to suppliers and partners.

If the Email system not operational it would be a major inconvenience but customers would still be able to register, deposit and wager – this would be a level 2 disaster situation, however since it is such a high profile function (i.e. senior management) it could be treated as a level 1 for political purposes.

The Live Chat system is also used by Customer Service to communicate to customers – if it was not operational this would be a level 2 (level tanımları yapıldı mı?) disaster situation.

4.2.3 Security incident / problem reporting

A local updated version of GITLAB is installed and used for problem reporting, issue management and tracking, software development code repository and planning. An immediate email is sent

to all members related to any subject upon issue assignment, new comments or status change. It is used extensively at TENV for the following purposes:

- Problem Reporting / Tracking / Issue management
- Security Incident Reporting / Tracking
- IT Software Development Methodology

Additionally email groups exist and all members have instant access to their emails (mobile, local or remote access). For urgent situations, a phone chain exists for quick response.

Microsoft Project is used for software development planning or issue management planning to define better timelines and resources.

If TENV was not operational it would be a very high Level 2 situation as it impacts so many areas in TENV, especially IT.

4.2.4 Third-party systems

There are a number of third party systems that are used to support the TENV:

If any of the above applications were not operational the disaster situation would be a level 2.

4.2.5 Financial system

The financial accounting package is **AccPac provided by Sage**.

4.2.6 Software Development System

Software development and maintenance is done by the IT Software Development team which consist of IT Manager, Frontend Developers, Backend Developers, Database Admins and Developers, Project Managers, Deployment Managers, Analysts.

Mainly there are four development environments.

New projects are created on Microsoft Project with a resource and time planning. These projects are assigned to Development team members using local Gitlab Issue and project management system. Project code repository is created on Gitlab and just projects members can access to that codes.

Existing projects are updated on Microsoft Project with a resource and time planning. These projects are assigned to Development team members using local Gitlab Issue and project management system. Project code repository is updated on Gitlab and just projects members can access to that codes.

- **DEV ENVIRONMENT:** This environment has a test database with the same structure of production database. Whenever a new project code is created or existing ones are updated, all codes are submitted to relevant code branches by developers immediately. All primary tests are carried out by the developers themselves.
- **TEST ENVIRONMENT:** Deployment Managers merges different code branches into Master branch to be deployed to TEST environment. All tests are carried out by the Team members , Project Managers and IT Manager, to check the correspondance with requirements.
- **STAGING ENVIRONMENT:** This environment uses production database but it is not for end users. All latest tests are carried out on this environent. This environment is pretty identical to production environment. All tests are carried out by the specified endpoint test users, team members , Project Managers and IT Manager, to check the correspondance with requirements.
- **PRODUCTION ENVIRONMENT:** If all tests were passed, projects are deployed to the Production Environment.

TC ENTERTAINMENT

5 TENV data backups / restore / test restore

5.1 Customer data

Customer data is maintained on the production network in Netherlands as MS SQL database.

There are a number of backups of the customer database. Four daily backups are scheduled. The first one is to be a full backup and the others are differential. And there is a secondary replication server with the same configuration. All data is replicated by SQL server mirroring feature for high availability.

And a new cluster is planned to consist at least three servers, one will be primary, the others will be instant secondary copies using latest version of SQL Server's advanced Always on High Availability features.

Backups for both primary database and secondary replication servers are copied to Head Office network for disaster recovery. Daily backups are kept in safe for 7 days prior to current day.

Production Network

- Replication by mirroring between primary and secondary data servers (real time)
- SAN1 – Database Backup (daily)

Disaster / Recovery Network

- Customer Database Replication (real time)
- SAN1 – Database Backup (daily)

In case of any failures at the Primary Data Server, the secondary replication server would change its role to be primary in seconds and Primary data server will be on restore mode until all data are synchronised between two servers. After full synchronisation is done, roles are switched again as before.

In case of any failures at the replication server in Netherlands, setup of replication server will be established again immediately.

In case of any failures at the production network in Netherlands, database is restored from latest backups on Head Office network and all the data traffic will be redirected to Head Office network.

Backups for database server located on Head Office network are scheduled to be four daily backups. The first one is to be a full backup and the others are differential. Daily backups are kept in safe for 7 days prior to current day.

If production network in Netherlands is accessible again, database server in Head Office network and in Netherlands will be synchronised by log shipping. And all data traffic will be redirected to Netherlands again.

5.2 Event / pricing data

5.3 Corporate data

5.4 Other data

Other important data on the TENV includes:

1. Source Code;
2. Documentation;
3. Logs;
4. Configuration Files;
5. Local GITLAB data
6. Voice Recordings.

5.4.1 Source code

Source code is maintained on a development server using GITLAB source code repository. Backups are taken daily.

5.4.2 Documentation

Documentation is maintained on a development server using Confluence. Backups are taken daily

5.4.3 Logs

System access logs, user access logs, database logs, etc are maintained on the central logging server. Secure Backups are taken daily.

5.4.4 Configuration files

Configuration files are maintained on the Central Logging server. Backups are taken whenever changes are made.

5.4.5 Local GITLAB Tickets

The local GITLAB tickets are maintained on the development server. Backups are taken daily.

5.4.6 Voice recordings

Voice recordings are maintained on the Central Logging server. Backups are taken daily.

6 Disaster recovery personnel

6.1 Disaster Response Management Team

The Disaster Response Management Team is responsible for:

- Reviewing a potential D/R situation
- Making a decision on whether to cutover to the D/R site
- Communicating situation to their staff
- Notifying suppliers, regulatory and shareholders
- Managing the disaster / recovery procedures established for their area

The Disaster Response Management Team consists of:

- Chief Executive Officer (CEO)
- Finance Director (FD)
- Chief Operating Officer (COO)
- IT Manager (IT)
- Network Manager (IT)
- Database Administrator (IT)
- Customer Service Manager (Customer Service)
- Operations Manager (Trading Floor)

The COO will coordinate and manage the disaster response management team.

6.2 TENV Departments

Risk Managers

The Poker Risk Manager is required for the response to the disaster situation and ideally five (5) trading floor operators should be available.

Customer Service

The Customer Service Manager and ten (10) Customer Service representatives are required for the response to the disaster situation

Information Technology

The entire IT department must be available for the response to a disaster situation. This will include:

- IT Manager
- Network Manager
- Application Development Manager
- Database Administrators
- Network Administrators
- Web and .Net Developers

Administration

The receptionist must be available for the response to a disaster situation.

Finance

Finance is required for the response to a disaster situation to ensure payroll and vendor payments are not interrupted.

Key Suppliers

The following is a list of the key suppliers that will be important in our response to a disaster situation:

- Payment Processors
- Financial packages supplier
- Poker system provider
- Leaseweb

6.3 Contact List

TC ENTERTAINMENT

7 Disaster / recovery situation assessment

If the situation occurs during normal working hours, IT staff will likely take the initial call. If situation occurs after normal working hours, the IT Emergency Support phone will be utilized and the after-hours support staff will take the call.

Either way the person taking the call will assess whether this is a critical situation and if they believe it is, they will call appropriate manager – Application Development Manager for application issues or the Infrastructure Manager for Infrastructure issues.

The Applications Manager or Network Manager will do their assessment and determine the severity of the situation. If it is a critical situation they will do the following:

1. A ticket is logged immediately into local Gitlab issue management system , otherwise notes are taken on the chronological events including times and any decisions made;
2. Contact IT Manager (if IT Manager is not available then the COO is contacted);
3. Initialize conference call:
4. If the IT Manager believes it will be a Level 1 situation he does the following:
 - Contacts the COO, CEO and FD;
 - Contacts Application Manager (if required);
 - Contacts Website Administrator (if required);
 - Contacts Network Manager(if required);
 - Contacts ITEX - providing the conference call information (if required);
 - Contacts Telecommunications company (if required) - providing the conference call information;
 - All required individuals join conference call, including Leaseweb.
5. All individuals join conference call;
6. The Applications Development Manager will ensure the appropriate unscheduled outage page is presented to our customers. If it is a Production network Level 1 then this will likely have to be hosted in a location other than the production network;
7. The IT Manager assesses the situation and determines if the Disaster Response Team should be involved at this time;
8. If the decision is affirmative then the IT Manager contacts the members of the Disaster / Recovery Response Team and asks them to join the conference call;
9. When the Disaster / Recovery Response Team joins the conference call, they are:
 - Updated on the incident
 - Informed of our options
 - Presented with our likely approach to resolving the problem
 - Possible resolution times
10. If it is determined that the outage cannot be resolved within 2 hours then a disaster situation is declared and depending on the disaster level, the appropriate Disaster / Recovery procedures are taken. This can be a guideline however it depends on the day of the week, the seriousness of the situation and how long it is estimated to restore operations;

8 Disaster / recovery / resumption procedures

8.1 Production network disaster situation

8.1.1 Production network – level 1 disaster

Once the Disaster Response Team have determined that this is a Level 1 disaster situation on the production network and action must be taken to transfer operations to the Disaster / Recover network, the following must happen:

1. The Website Administrator will update the unscheduled outage page with a possible resolution time;
2. The Department Managers will inform their staff of the Level 1 situation and ensure they follow any departmental disaster recovery procedures, including informing IT immediately of any anomalies once the disaster / recovery network is operational;
3. The IT Manager will inform Leaseweb to switch the IPs to the Disaster / Recovery network;
4. The IT Manager will ensure that the Disaster / Recovery network operational and that the database is up-to-date to the point of the production network failure;
5. The IT Manager will ensure that the Customer Verification process is operational;
6. The IT Manager will ensure that the Payment Processors are operational on the Disaster / Recovery network, including some test deposits;
7. The Database Administrator will ensure that the database integrity has been maintained and that the data has not been lost in the switchover;
8. The Disaster / Recovery site is fully tested to ensure it is operational and if it is then the Website Administrator will take the unscheduled outage page down;
9. Leaseweb will change the IP address to point to the Disaster / Recovery network
10. The Database Administrator will synchronize the databases before D/R production site access is established.
11. Customers will start access the D/R site;
12. In the meantime, the IT team & Leaseweb will work on resolving the problem;
13. Once the problem has been resolved then a switch back to the primary production begins;
14. The Application Development Manager will ensure that the Production network is operational again;
15. Manager will inform Leaseweb to switch the IPs back to the Production network;
16. The IT Manager updates the ticket that was created in local the Gitlab issue management system with the details of the solution implemented and a summary of the situation and impact of the situation;

8.1.2 Production network – level 2 disaster

If the Disaster Response Team has determined that this is a Level 2 disaster situation on the production network, then there is no need to transfer operations to the disaster / recovery site. The situation is isolated to a non-critical application or network infrastructure issue.

The Department Managers will inform their staff of the Level 2 situation and ensure they follow any departmental disaster recovery procedures, including informing IT immediately of any anomalies, once the situation is resolved;

The IT Manager will assign the resolution of the situation to the appropriate IT resource;

The IT Manager will communicate the status of the Level 2 situation to the Department Managers every two (2) hours;

Once the Level 2 situation is resolved, the IT resource assigned to the situation updates the ticket that was created in local the Gitlab issue management system with the details of the solution implemented and provides a summary of the situation and impact of the situation;

9 Test disaster / recovery plan

9.1 Test production network disaster recovery plan

9.2 Test head office network disaster recovery plan

10 End of document

End of Document

TC ENTERTAINMENT