Business Continuity Plan

Policy No: 1.0.0	**Effective:** 19-12-2022
Prepared by: Stephan Csorba	**Approved by:** Hans van Veggel

Confidentiality Statement:
The information contained in this document is privileged and confidential and protected from disclosure outside E-WISE The recipient is hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited without the prior written approval from the director of E-WISE.

Establishment Date:	19-12-2022		e-WISE Good To Know
Revision Date:	19-12-2022	Business Continuity Plan	
Revision Number:	1.0		

Revision history

Revision	Author	Date	Reviewer	Date	Comments
1.0	Stephan Csorba	19-12-2022	Hans van Veggel	19-12-2022	No comments
1.1	Johan Assen	02-12-2024	Stephan Csorba	02-12-2024	- Replaced Crisis manager

The purpose of the Business Continuity Plan is to define precisely how E-WISE will manage incidents in the case of a disaster or other disruptive incident, and how it will recover its activities within set deadlines.

The objective of this plan is to keep the damage of a disruptive incident at an acceptable level. This plan is applied to all critical activities inside the scope of the Information Security Management System (ISMS).

Users of this document are all staff members, both inside and outside the organization, who have a role in business continuity. This policy revision 1.0 will come into effect from 13-06-2022.

Name: Stephan Csorba

Designation: Stephan Csorba

Signature: ___________________

Date: _______________________

Chapter 1 Reference documents

- ISO 22301 standard, clause 8.4
- ISO 27001 standard, clause A.17.1, A.17.1.2, A.17.1.3
- List of Legal, Regulatory, Contractual and Other Requirements
- IT Security Policy
- IT Impact Analysis
  - Studio
  - IT

Chapter 2 Business Continuity Plan

Section - 2.1 Plan content

The Business Continuity Plan consists of these major parts:

- Business Continuity Plan – defines top-level rules for business continuity
- Incident Response Plan – Appendix 1 – a plan that defines solutions for direct response to the occurrence of various types of incidents
- Disaster Recovery Plan – a plan that defines solutions for the recovery of IT infrastructure and IT services
- Recovery plans for individual activities - these are prepared separately for each activity - Appendix 6 and on - plans dealing with the solutions for recovery of necessary resources for each activity

Each of these plans defines its activation procedure.

Section - 2.2 Assumptions

For this plan to be effective, all the resources and arrangements specified in the Business Continuity Strategy need to be prepared.

Section - 2.3 Appointments and authorities

The following bodies are formed when a disruptive incident occurs:

Crisis Management Team		
Members:	Substitutes:	Role:
Operational Director	Board of Directors	- Activate/Deactivate Business Continuity Plan - Manage internal communication with employees.

		- Manage press releases, social communication etc.
CTO Reducate	ISSC	- Activate/Deactivate Business Continuity Plan - Authorize purchase up to € 100K - Coordinate IT tasks from Business Continuity Plan
Crisis Management Support Team		
Members:	Substitutes:	Role:
ISSC (Recovery managers)	Senior IT-managers	- Coordinate IT tasks from Business Continuity Plan
Marketing Manager	Board of Directors	- Deliver messages and materials for press releases, social communication etc.
Managers	Senior Employees	- Manage internal communication with employees.

The purpose of the Crisis Management Team is to make all key decisions and coordinate actions during the disruptive incident; the purpose of the Crisis Management Support Team is to relieve the Crisis Management Team from administrative and other operational activities, in order to focus on managing the disruptive incident. Members of the Crisis Management Support Team are directly responsible to the Crisis Management Team.

Recovery managers for individual activities are appointed in the recovery plans for the said activities.

Authorizations for action during disruptive incident are the following:

Type of decision	***Who is authorized***
How small incidents related to IT and communications technology are resolved	Employees in ISSC
How all other small incidents are resolved	Employees in ISSC
Making a decision about invoking recovery plans	Operational Director
Making a decision about the selection of alternative site (use of close or remote alternative site)	Operational Director
Informing employees about the invocation of recovery plans	Operational Director; if he/she is unable to do it, then recovery manager for individual activity
Implementing all tasks necessary for the recovery of individual activities	Recovery Manager for individual activity
Content of the communication for different interested parties	Operational Director
Selecting information to be provided to the public media during disruptive incident	Marketing Manager
Purchases during disruptive incident - over € 100K	Management Reducate
Purchases during disruptive incident - up to € 100K	Management Reducate

Section - 2.4 Plan activation; plan deactivation

The Incident Response Plan is activated automatically in case an incident occurs, or a potential incident is threatening its activities. The Incident Response Plan is deactivated after an incident has been contained or eradicated.

Disaster Recovery Plan and recovery plans for particular activities are activated exclusively by the Operational Director’s decision, if he/she assesses that a particular activity will be interrupted for a period longer than the recovery time objective for that activity. The decision of the Operational Director may be written or oral.

Disaster Recovery Plan and recovery plans may be deactivated by recovery managers for individual activities when they establish that all conditions for the resumption of business activities have been met. Disaster Recovery Plan and recovery plans are deactivated by resuming normal business activities.

Section - 2.5 Communication

The following means will be used for communication between the Crisis Management Team and activities, and between activities themselves - they are ordered according to priority (the first one from the list is to be used first; in case it is not available, the next one is used):

Affects e-learning environment (See appendix 7 - communication templates)

1. A status page
2. Chat tool
3. Email
4. Social media
5. Press release

Affects internal operations (See appendix 7 - communication templates)

1. ZOHO Ticket system
2. Email
3. Phone
4. Chat tool

Operational Director & CTO Reducate in the Crisis Management Team are responsible for coordinating communication with all activities.

Responsibilities for communicating with particular interested parties, including the public media, are specified in the Incident Response Plan.

Section - 2.6 Sites and transportation

The HR-Department is responsible for ensuring access to each provided alternative site. Appendix 3 – List of Business Continuity Sites specifies all provided alternative sites.

Responsibilities for transportation to alternative sites are specified in Appendix 4 – Transportation Plan.

Section - 2.7 Order of recovery for activities

Activities must be recovered in the following order:

No.	***Name of activity***	***Recovery time objective***
1	E-learning environment	4 hours
1.1	Web hosting	1 hour
1.2	Data restore	2 hours
1.3	Test & go live	1 hour
2	CRM Cloud system	4 hours
3	Internal operations	
3.1	IT Department	1 hour
3.2	Studio Department / Studio’s	24 hours
3.3	Production Department	24 hours
3.4	Sales Department	48 hours
3.5	Finance Department	48 hours

Section - 2.8 Interdependencies and interactions

The dependencies and interactions between activities, as well as with suppliers and external parties, are detailed in the Incident Response Plan, the Disaster Recovery Plan, and individual recovery plans for activities.

Section - 2.9 Required resources

Resources that are required for the recovery of the activities are listed in their recovery plans; the resources required for the recovery of IT infrastructure and IT services are listed in the Disaster Recovery Plan.

The Command Centre, which serves the Crisis Management Team and Crisis Management Support Team, is equipped as follows:

Name of resource	***Description***	***When the resource is necessary***	***Person responsible for obtaining the resource***
Applications / databases:			
E-learning environment	Our customer portal	[within 4 hours]	CTO Reducate
CRM Cloud system	Our internal system for all departments	[within 4 hours]	CTO Reducate
Data in electronic form:			
Business Continuity Strategy and plans for all activities		immediately	Operational Director
Data in paper form:			
Business Continuity Strategy and plans for all activities		immediately	Operational Director
IT and communications equipment:			
Workstations		[within 24 hours]	System Administrator
Telephones	Cloud based 3CX	immediately	System Administrator
Mobile phones	Sales department only have mobile phones	immediately	IT-Department
Communication channels:			
Telephone land lines	Cloud / 3CX	immediately	System Administrator
Internet access	Eurofiber	[within 2 hours]	System Administrator
Facilities and infrastructure:			

Production Facilities / Studio’s	Our studio’s need to work in another facility	immediately	Studio department
Office space	Our staff can work in the cloud / home	[within 1 month]	HR-Department
Computer network		[within 24 hours]	System Administrator
Office equipment		immediately	HR-Department
External services:			
Electricity	Meac vastgoed	immediately	HR-Department

Chapter 3 Restoring and resuming business activities from temporary measures

The purpose of restoration and resuming the business activities from temporary measures is to bring the business operations back to business-as-usual – to the normal state as it was prior to the disruptive incident.

The steps described in this section are not time critical – they are to be performed in proportion with the impact of the disruptive incident and in accordance with available resources. The decision to activate each of the following steps is made by the Operational Director.

The following steps need to be performed, in this order:

1. Preservation of the damaged assets and evaluation of damage
2. Assessment of the situation and determining options and responsibilities
3. Developing an action plan – determining the steps needed to return activities to normal state

Section - 3.1 Preservation of damaged assets and evaluation of damage

The board of directors, IT-director or ISCC will nominate the team for preserving the damaged assets – the focus of this team is to prevent the damage from spreading.

The board of directors, IT-director or ISCC will nominate the team for evaluation of damage. The evaluation must consist of the following: name of the asset, location of the asset, type of damage, and cost of damage.

Section - 3.2 Assessment of the situation & determining options and responsibilities

Depending on the extent of the damage, the Operational Director needs to decide the following: (1) whether to move back to the primary location or look for a new location, (2) whether to purchase new equipment or repair the existing, (3) when and where the operations of activities that do not support key products and services (activities with lower priority) will be recovered/resumed, and (4) whether there are enough human resources to support normal operations, etc.

Based on these decisions the Operational Director must nominate responsible persons for the following:

a) Making claims against insurance policies
b) Restoring facilities
c) Acquiring new facilities
d) Logistics for moving to other locations
e) Repairing the equipment
f) Purchasing new equipment
g) Hiring new personnel
h) Recovering lower priority activities

Section - 3.3 Developing action plans

Each responsible person must develop an action plan for his/her area of responsibility, which will – amongst other information – contain the following: (1) steps to be taken, (2) required human resources, (3) required financial resources, and (4) deadlines.

The Operational Director must define (1) how to provide necessary funding, (2) procurement process and authorizations, (3) which reports will be sent to the Crisis Management Team, and (4) who will perform the review of the steps once they are completed.

Chapter 4 Validity and document management

This document is valid as of 19-12-2022.

This document is stored in the following way:

- The paper form of the document is stored at the following locations: Command Centre, HR-Department.
- the electronic form of the document is stored in the following way: Google Drive

The owner of this document is Stephan Csorba, who must check and if necessary update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Did activities recover within required time?
- Are recovery plans and Incident Response Plan synchronized?
- Did exercising and testing achieve objectives?

Chapter 5 Appendices

Appendix 1 – Incident Response Plan
Appendix 2 – Incident Log
Appendix 3 – List of Business Continuity Sites
Appendix 4 – Transportation Plan
Appendix 5 – Key Contacts
Appendix 6 – Disaster Recovery Plans

Appendix - 1 Incident Response Plan

Incident	***Response plan***
IT and communications equipment:	
Data leakage (GDPR)	● https://docs.google.com/document/d/1DzsbpbQUm1JuO-ML6LMjpjoZU-qLmtp6Olnkr82UBuA/edit ● Contact insurance company (Appendix 5)
AWS Servers Down (E-learning)	● Contact vendor inQdo https://docs.google.com/document/d/17OK70JPoQQhLIAQHvLvf9XV4QR-Optm1/edit#
Marketing Websites Down	● Contact vendor Platform.sh by ticket or account manager (Appendix 5)
Zoho One CRM Down	● Contact vendor Tactick by ticket or account manager (Appendix 5)
Computers affected with malware	● Contact IT-Department
Facilities and infrastructure:	
Internet access	● Contact Eurofiber (Appendix 5)
Facility security (burglary)	● Contact external security company (Appendix 5) ● Contact insurance company (Appendix 5)
Facility disasters, fire, water damage etc.	● Local authorities, police, fire department, call 112 ● Building owner (Appendix 5) ● Contact insurance company (Appendix 5)
External services:	
Electricity	● Building owner (Appendix 5) ● Contact insurance company (Appendix 5)

Appendix - 2 Incident Log

Incident	***Registration of incident(s)***
IT and communications equipment:	
Data leakage (GDPR), AWS Servers Down, Marketing websites down, Zoho One CRM Down, Computers affected with malware	ZOHO Projects SIEM, by e-mail or: https://docs.google.com/document/d/1rMvohFkxB-h0NfbVtEPkZu5V5KBS45SUqEKXH6FFgY8/edit
Facilities and infrastructure:	
Internet access, Facility security, Facility disasters, fire, water damage etc.	ZOHO Projects SIEM or if not accessible register by email.

Appendix - 3 List of Business Continuity Sites

Name of activity	***Recovery time objective***
Studio 1	**Studio Stream** Maarssenbroeksedijk 2C 3542 DN Utrecht 0346 550 531
Studio 2	**Camfactor** Atoomweg 280 3542AB Utrecht +31 85 30 30 700

Appendix - 4 Transportation Plan

Transportation costs can be declared at the finance department. No transportation plan is needed because all employees except for the Studio Department (appendix 3) can work from home in the cloud.

Appendix - 5 Key Contacts

Board of directors	**Stephan Csorba** IT-Director / Security officer (ISSC) 030-2644110 06-14745710 stephan.csorba@e-wise.nl **Ellen Smit** Operational director 030-2644109 06-52334479 ellen.smit@e-wise.nl **Marjolein van Agtmaal** Finance Director 030-2644102 06-46084148 marjolein.van.agtmaal@e-wise.nl
IT and communications equipment:	
Data leakage (GDPR)	**Board of directors** https://datalekken.autoriteitpersoonsgegevens.nl/
AWS Servers Down (E-learning)	**inQdo B.V.** Coltbaan 1-19, 3439 NG, Nieuwegein 085 201 1161
Marketing Websites Down	www.platform.sh **Rohan Nair (accountmanager)** rohan.nair@platform.sh
Zoho One CRM Down	**Tactick** Vendelier 71c, 3905 PD, Veenendaal 085 001 3687
Facilities and infrastructure:	
Internet access	https://www.eurofiber.com 030 242 8700
Facility security (burglary)	**Cees Groeneveld - inzake pand** groeneveld@meacvastgoed.nl 06 5473 3812

	BBN Beveiliging BV 0346 – 552507 **See insurance contact**
Facility disasters, fire, water damage etc.	112 **Cees Groeneveld - inzake pand** groeneveld@meacvastgoed.nl 06 5473 3812 **See insurance contact**
External services:	
Electricity	**Cees Groeneveld - inzake pand** groeneveld@meacvastgoed.nl 06 5473 3812
Insurance	**Robert van Duijn** **Account manager** 06 - 11 53 08 31 rvanduijn@klap.com **Jurgen van Veenendaal** **Inkomen consultant** 020 - 261 61 81 jvanveenendaal@klap.com
More contacts	**See ZOHO One CRM - Partners**

Appendix - 6 Disaster Recovery Plans

1. E-WISE - E-learning environments
2. E-WISE - Marketing websites
3. ZOHO One
4. Exact Online
5. BCS Online
6. Routers & switches internal
7. Desktops & laptops
8. AFI Google Drive

Appendix - 7 Communication templates

Please find below a list of different communication templates.

1. E-mail
2. Social Media
3. Website
4. Press release

Data leakage - email, social media, website, press release

Dear valued customer,

We regret to inform you that we have recently discovered a data leakage incident that may have compromised some of your personal information. We take our responsibility to protect your data very seriously and are taking immediate action to address the situation.

We are currently working with law enforcement and cyber security experts to fully assess the extent of the data leakage and take all necessary steps to prevent similar incidents from happening in the future.

We want to assure you that we have already taken steps to secure our system and have implemented additional measures to safeguard your data.

We deeply apologize for any inconvenience this may have caused and are committed to keeping you informed as we continue to investigate this matter. If you have any further questions or concerns, please do not hesitate to contact our customer support team.

Thank you for your understanding and support during this challenging time.

Sincerely,

[Company Name]

Website down - email, social media, website, press release

Dear valued customer,

We are writing to inform you that our website is currently experiencing technical difficulties and is temporarily unavailable. We apologize for any inconvenience this may have caused and are working diligently to resolve the issue as soon as possible.

Our team of experts is currently investigating the cause of the outage and working to restore access to the website as quickly as possible. We understand how important our website is to you and we appreciate your patience and understanding during this time.

In the meantime, if you have any urgent needs or questions, please do not hesitate to contact us by phone or email. Our customer support team is available to assist you and will do their best to answer any questions you may have.

We will continue to keep you informed of the situation and provide updates as soon as we have them. We apologize again for any inconvenience this may have caused and appreciate your patience and understanding during this time.

Sincerely,

[Company Name]

Website maintenance - email, social media, website, press release

Dear valued customer,

We are writing to inform you that our website is currently undergoing scheduled maintenance and will be temporarily unavailable during this time. We apologize for any inconvenience this may cause and appreciate your patience and understanding.

During this maintenance period, our team will be working to improve our website's functionality and ensure that it remains secure and up-to-date. We expect the maintenance to be completed within the next [insert time frame] and will notify you once the website is back up and running.

If you have any urgent needs or questions during this time, please do not hesitate to contact us by phone or email. Our customer support team is available to assist you and will do their best to answer any questions you may have.

We appreciate your patience and understanding during this maintenance period. We look forward to providing you with an even better website experience once the maintenance is complete.

Sincerely,

[Company Name]