ECSEL-ED-2015-065

DECISION ECSEL-ED 2015-065 OF THE EXECUTIVE DIRECTOR

Relating to the Business Continuity and Disaster Recovery Plans of the ECSEL JU

THE EXECUTIVE DIRECTOR OF THE ECSEL JOINT UNDERTAKING,

Having regard to the Financial Rules of the Joint Undertaking (ECSEL-GB-2014-09), and in particular Articles 11, 12 and 17,

Having regard to the Decision of the Governing Board adopting the requirements for the Internal Control Standards of the Joint Undertaking (ECSEL-GB-2014-15).

Whereas:

(1) The Governing Board has adopted a set of Internal Control Standards (ICS) including ICS 10 relating to business continuity and stipulating that "adequate measures are in place to ensure continuity of service in case of 'business as usual' interruptions, and that plans are in place to ensure that the Joint Undertaking (JU) is able to continue operating to the extent possible whatever the nature of any major disruption.

(2) It is the duty of the organisation to develop its ICS implementation plan and in particular to ensure the efficiency of its business continuity while at the same time updating tools and methods which prove to be necessary.

(3) The Commission has, on 23 April 2015, provided the JU with substantial support in dealing with disaster recovery plans of the JU which constitute a key element of the business continuity plan.

Has decided,

Article 1

The Business Continuity Plan (BCP) of the ECSEL Joint Undertaking (version 3.0 validated on 01 June 2015), as attached in Annex 1, is hereby approved.

Article 2

The Business Continuity Plan mentioned in Article 1, is communicated to the staff.

Done in Brussels, on 01 June 2015

Andreas Wild
Executive Director

Annex: BCP version 3.0 validated on 01 June 2015

ECSEL JU

BUSINESS CONTINUITY PLAN

- Version 3.0 –

Version Control	**3.0**
Validated by	**Wild Andreas**
Date of validation	**01/06/2015**
Maintenance	**Hanane El Fatmi**
Stored location	BC Desk Officer

CONTACTS

ECSEL DUTY OFFICER	**Hanane El Fatmi** **+32 (0) 2 221 81 01**
ECSEL MAILBOX	**ECSEL@ECSEL.europa.eu**
ECSEL WEBSITE	**http://www.ECSEL.eu/**
ECSEL BC Correspondent	**Marc Jeuniaux** **Marc.Jeuniaux@ecsel.europa.eu** **+ 32 (0)2 221 8110** **+ 32 (0)474 367 896**
ECSEL BC Desk Officer	**Hanane El Fatmi** **Hanane.El Fatmi@ecsel.europa.eu** **+ 32 (0)2 221 81 01** **+32 (0) 498 98 42 34**
TO56 Chef d'immeuble	**Knight Franck – Aurelie Borgniet - 0495 41 49 03**
Commission DS	EC-SECURITY-AND-SAFETY@ec.europa.eu EC-SECURITY-CRISIS-ROOM@ec.europa.eu EC-SECURITY-ARGUS@ec.europa.eu
Commission ADMIN/DS DUTY OFFICER	+32 (0)2 29 22222
Commission SG DUTY OFFICER	+ 32 (0)498 980255
Commission DIGIT CENTRAL HELPDESK	+ 32 (0)2 29 58181
Commission CNECT DUTY OFFICER	0498 98 99 00 / 0498 98 99 01
Commission CENTRAL MAIL SERVICE	OIB-COURRIER-CENTRAL-MAIL@ec.europa.eu +32 (0)2 29 51896

DOCUMENT HISTORY

Version	Date	Comment
1.0	27/01//2015	First draft
2.0	20/04/2015	Second draft
3.0	05/05/2015	Final

TABLE OF CONTENTS

1. INTRODUCTION

The Decision ECSEL-GB-2014-15 of 03 July 2014 of the Governing Board has established the internal control standards for effective management.

Internal control standard 10 (ICS 10) is stipulating that adequate measures are in place to ensure continuity of services in case of "business as usual interruption".

On 17 January 2011, the predecessors of the ECSEL JU, ARTEMIS and ENIAC Jus, moved to the actual location of ECSEL in the premises situated in the building TO 56, shared with 4 other Joint Undertakings (IMI+FCH+Clean Sky from the beginning, then BBI and Shift 2 rail in 2015).

The ECSEL Business Impact Analysis was approved by the ECSEL management team and on that basis the Business Continuity Plan (BCP). has been established. The BCP was discussed and adopted on 07/05/2015 by the JU's management and has been transmitted to the Commission – DG CNECT and to the other 5 JUs sharing the office location in the building TO 56.

The BCP has been updated to take into consideration the ongoing risk assessment analysis and the outcome of the discussions and interaction between actors involved, in particular with regard to the definition and implementation tools and methods to be put in place in case of disaster in the premises, and with consolidating the support solutions made available recently by the services of the Commission.

2. PURPOSE AND SCOPE OF THE ECSEL BCP

The purpose of this BCP is to enable ECSEL to recover or maintain its activities in the event of a disruption to its normal business operations. It is a collection of the procedures to be followed and information for use following a crisis incident. The BCP is only applicable to a major disruption/crisis at JU level, and addresses the JU's *Critical Functions*. The BCP is a working document which will be reviewed and updated on the basis of the results of BC exercises and/or on a regular basis (at least once a year by the BC Desk Officer). The annexes will be updated whenever necessary.

3. CRITICAL FUNCTIONS

The critical functions identified in the ECSEL JU Business Impact Analysis are:

- **JU management and decision taking including crisis management**
- **Internal communication (including Human Resources)**
- **External communication**
- **Maintaining IT support (systems and infrastructure)**
- **Administrative expenditure – payment processing**
- **Financial management and Accounting**

In case of an incident, the highest priority will be given to maintaining these functions or, in case of a disruption, to restore them within 48 hours to an acceptable level. Other functions of ECSEL JU will be executed on a best effort basis.

4. ROLES AND RESPONSIBILITIES

4.1. Crisis Management Committee (CMC)

The CMC is responsible for the first intervention in case of incidents and for activating the BCP when necessary. Members of the CMC will receive the first call (through the BC Desk Officer typically) or be present at the moment of the incident. They are empowered to take immediate decisions as to actions to be undertaken to contain damages.

The CMC is headed by the Executive Director (or in case of his absence alternatively by the Head of Administration) as Chairman and is comprised of the management team, the BC Correspondent and BC Desk Officer. The Committee is supported by a secretariat. The composition and contact details of the CMC are shown in Annex I.

The role of the CMC is to:

- Assess the crisis level, in co-ordination with Commission-wide crisis groups, if required;
- Activate the BCP in ECSEL;
- Decide on immediate recovery actions;
- Give instructions to the members of the team;
- Take all relevant decisions in order to avoid threats to staff, services and property;
- Steer the recovery process;
- Monitor the evolution of the crisis response;
- Activate ECSEL's internal communication channels (including call cascades);
- Communicate to stakeholders;
- Liaise with the Commission services involved (in particular DG CNECT, SG, DG BUDG, DG ADMIN, OIB, PMO) and other service providers.

The CMC is responsible to ensure proper coverage of the critical functions identified:

- Internal Communication and Human Resources
- External Communication
- IT Infrastructure and Systems
- Finance, Budget and Accounting

The task of the CMC is also to:

- Ensure the recovery of the service's critical functions within 48 hours;
- Log all important actions and decisions;
- Perform a post-crisis review.

4.2. BC Correspondent:

The BC Correspondent is responsible for ensuring the ECSEL JU's preparedness by:

- Coordinating the creation of a BCP;
- Initiating updates of the BCP and contact details in the BCP;
- Planning BC exercises;

The BC Correspondent is member of the Crisis Management Committee.
ECSEL BC Correspondent: Marc Jeuniaux, back-up: Juan Pablo Contreras

4.3. BC Desk Officer:

The BC Desk Officer provides support to the BC Correspondent by:

- Forwarding proposals for the preparation of the BCP;
- Ensuring that documents, procedures and contact lists are up-to-date;
- Representing the ECSEL JU at the Business Continuity Network (BCN);
- Creating awareness amongst staff;
- Executing BC exercises;
- Training staff and management.

ECSEL BC Desk Officer: Hanane El Fatmi, back-up: Benedicte Van der Beke

5. BCP OPERATIONAL PROCEDURES

The operational procedures for the Business Continuity Plan cover two scenarios:

1. **Predictable or "creeping" crises** such as outbreak of disease or pandemic;
2. **Sudden impact crises** such as the loss of a building, infrastructure or key staff through fire, terrorist attack or major system breakdown with little or no warning, which may happen during or out of normal office hours.

(Potential) crisis situations are managed following the evaluation of the gravity of the event and its effect on ECSEL's functions and responsibilities:

WHITE	No particular threat.
YELLOW	Potential threat (e.g. small fire breaks out in the near environment of the ECSEL JU, but does not affect any of the JU's assets or building, or international/national alert on pandemic).
ORANGE	Threat (e.g. small fire in the building or pandemic affecting staff in the EU Institutions).
RED	Serious Threat (e.g. fire in the offices of the JU and pandemic affecting ECSEL JU's staff).
GREEN	Recovery after a crisis.

In a foreseeable crisis, different stages may occur with different timings and even with time lapses in between (e.g. a pandemic which follows different stages: alerts by the WHO, national health authorities, actual break-out of the disease, different waves of a pandemic). During a sudden crisis, these different stages cannot necessarily be

distinguished from each other and the "RED" situation is therefore almost always directly applicable.

As each crisis is different, with aspects that are difficult or impossible to anticipate, the following procedures are to be considered as guidelines only.

5.1. Operational Procedures for Crises

For creeping crises (typically pandemic), the main input will come through the Business Continuity Network (BCN) put in place by the 5 JUs sharing the premises and composed of the 5 BC Desk Officers also involved in the implementation of the common security policy in the TO 56. In crisis situations, any BCN member must act as soon as recognizing the need in on behalf of the whole BCN.

Input may also come via the ARGUS[1] system. ARGUS is a general rapid alert and response system established by the Commission, in order to enhance the capacity of the Commission and EU services to provide a quick, efficient and coherent response in the event of a major crisis of a multispectral nature, covering several policy areas requiring action at Community level, whatever its cause.

The BCN shall address a formal request to the Commission to be included in the ARGUS system with a view to accelerate the exchange of information in case of crisis by sending an email to the COMMISSION DS at EC-SECURITY-ARGUS@ec.europa.eu.

On the other hand, incidents that may lead to a sudden crisis are normally detected by staff members of the ECSEL JU or other JUs, the Service Managers or the BC Desk Officer.

Procedures applicable to the two types of crises are principally the same. Only the timing may differ from one type of crisis to the other. Progress from one stage to the other is formalized by a decision by the CMC.

5.1.1. Stage 1 (Code White)

Stage 1 (Code white - the normal stage) is used to review operational BCP procedures and to test the crisis management procedures.

5.1.2. Stage 2 (Code Yellow)

Stage 2 (Code yellow - (pre-) alert stage) indicates a stage in which there is a potential threat (usually only applicable in case of creeping crises) to the BC. (Additional) measures are taken to ensure preparedness.

5.1.3. Stage 3 (Code Orange)

Stage 3 (Code orange – high alert stage) - the message will be received from the BCN or the building manager/*chef d'immeuble* by the ECSEL BC Desk Officer. The BC Desk Officer informs the Executive Director (or in case of his absence, the Head of Administration) The BC Desk Officer and the Executive Director shall take decisions in relation to the immediate containment of damages and decide on the convocation of the CMC. The Chairman of the CMC will call for a meeting within 24 hours at the latest and will either meet physically in the JU's premises, if possible, or otherwise in the meeting point agreed and notified in the security rules and instructions. There will be at least one CMC meeting every week during this stage. In addition, the CMC will verify that all crisis management and business continuity procedures are in place and that the staff identified as essential is correctly informed. The CMC will decide on the activation of the BCP, and the communication measures

[1] OJEU L 19 OF 24.01.2006 PAGE 20.

to staff, relatives, Commission services concerned and other stakeholders, contractors and beneficiaries. Stage 3 may last from several days to several months.

5.1.4. Stage 4 (Code Red)

Stage 4 (Code red – crisis stage) – is announced by the CMC at the first sign that essential ECSEL JU's functions are affected by the crisis, or if the message is received from the BCN that the ARGUS Crisis Cell invites Services to launch their BCPs. The Chairman of the CMC will call a CMC meeting as soon as possible and declare a crisis Stage 4. The CMC activates the BCP and will meet at least daily at a fixed hour. For the rest of the day, the BC Desk Officer will be the main contact point. Special meetings may be held on specific issues as they arise. After the first week of stage 4, the CMC will decide on the future frequency of meetings. The CMC secretariat, together with the BC Desk Officer, will prepare the briefing of the daily meeting, summarizing information available in the ECSEL JU and information received from the Commission or other public/private services involved, with presenting decisions to discuss and take. (See standard briefing agenda in Annexes 2 & 3). Stage 4 may last several weeks.

5.1.5. Stage 5 (Code Green)

Stage 5 (Code green recovery stage) - as soon as the BCN informs the ECSEL JU that ARGUS has declared the end of stage 4 (Code Red) or if the level of staff present at work exceeds 80% or in any other case sufficient recovery operations have started, the CMC will decide to move to stage 5 (Code Green). During this stage, suspended services and actions will progressively be resumed and the backlog absorbed. The CMC will meet on a weekly basis to review progress or may decide to dissolve and to handover for discussion at the management meeting. Stage 5 may last for several weeks/months. At the end, the crisis level will return to normal (stage 1 - Code White).

6. INTERNAL AND EXTERNAL COMMUNICATION

Communication is an important element before and during a crisis situation.

6.1. Communication before a crisis

It is important to provide staff with information on what to do and how to obtain information in the event of a crisis before it actually occurs. This will be done through a Crisis Communication Plan (CCP) and crisis page on the ECSEL shared drive, as well as through a presentation to all staff and simulation exercises.

Being duly prepared will help to ensure that JU's staff has access to information that is relevant to their role before, during and after a crisis.

6.2. Communication during a crisis

Given the inherent nature of a crisis situation, which often leads to the temporary breakdown of normal channels of communication and physical dispersal/unavailability of key personal, key features of the internal communication plan are:

- A multi-channel approach to ensure that messages get through;
- Automation of notification systems as far as possible to avoid any delays;

- In-advance preparation of messages/websites/communication tools

Communication is vital during the crisis (Stage 4 – Code Red), in order to inform staff whether to come to the office or not and to inform staff and relatives periodically about what is going on and communicate decisions by the CMC. Also communication to the media and beneficiaries and contractors could be of relevance.

During the recovery period (Stage 5 – Code Green), it will be necessary to inform staff periodically on what the progress is, communicate decisions through the CMC, communicate to stakeholders and beneficiaries, as well as possible communication to the media, beneficiaries and contractors.

Details are given in the Crisis Communication Plan and its communication templates (Annex 4).

In the event of a crisis, the BC Desk Officer will be the first person informed.

Outside of office hours: the BC Desk Officer will be the first person informed by security services, police, fire department, contact persons of other EC services. The BC Desk Officer will immediately inform the Executive Director or, in case of the Director's absence, alternatively the Head of Administration/Head of Programmes will be contacted.

7. SECURITY MEASURES AND ALTERNATIVE OPERATIONAL SITES

The ECSEL Joint Undertaking currently operates in the TO 56 building, designated as "White Atrium" situated at Avenue de la Toison d'Or 56-60, in Brussels.

- CODE WHITE

No particular threat – normal situation and normal security measures applicable.

- CODE YELLOW

In case of a Code Yellow crisis, in which the building infrastructure is not affected (e.g. small fire breaks out in the near environment of the JU, nearby manifestations or riots etc), the JU will continue to operate in its premises and to co-ordinate the crisis from there in liaison with the building manager/*chef d'immeuble*.

The TO 56 Chef d'ímmeuble (in cooperation with the competent services of the Commission HR-.DS) will enforce the following security measures:

- Reinforcing security of staff where necessary.
- Limiting, where appropriate, the number of access points to building reception areas and/or garages.
- Denying access to visitors' vehicles.
- Reinforcing access controls: checking valid access passes, checking delivery of goods to storage and meetings areas, conducting visual checks of vehicles and hand luggage of any person about whom there are suspicions.

- CODE ORANGE

In case of a Code Orange crisis, (e.g. small fire in the building) "business as usual" will be severely curtailed.

- Non-essential activities which may place staff at risk will be postponed.
- Access to the JU's premises will be limited to service cardholders and denied to all visitors.

- Opening hours of premises will be restricted and garages closed except to service cars.
- A risk assessment may lead to evacuation of the building considered vulnerable.

• CODE RED

In case of a Code Red crisis, (e.g. building and infrastructure becoming inaccessible for a long period) a fully equipped back-up building will have to be identified in coordination with the above mentioned services of the Commission.

Depending on the duration of the crisis period, the back-up building will have to provide shelter for the CMC team and/or for the JU staff able to work.

Until a secure back-up building is available and depending on the nature and severity of the threat, staff will be given instructions on the actions expected of them and how critical activities are to be maintained whilst respecting the following safety precautions:

- Non-essential activities which may place staff at risk are cancelled.
- Risk assessment and safety precautions may prohibit staff from congregating together in large groups.
- Access to the ECSEL JU's premises will be denied to all visitors and deliveries by external contractors will be prohibited.
- Garages will be closed to all cars.

• CODE GREEN

When a Code Green stage is reached (recovery stage), certain enforced security measures may remain in place (see measures under "Code Yellow").The ECSEL JU will restore its usual activities in the measure and timing possible either from its usual premises or temporary premises and co-ordinate the recovery actions from there in liaison with the building manager/*chef d'immeuble*.

Whenever the JU's activities are fully recovered, the CMC will announce the "Code White" or "back to business as usual" stage.

8. DOCUMENT MANAGEMENT ARRANGEMENTS

In case of Code Orange and Code Red crises and following evacuation of the building, the Commission's Central Mail Service will have to be alerted in order to keep the JU's inbound mail until a new delivery address has been identified. Stakeholders will have to be informed and asked to postpone non-critical mail shipments.

Following a crisis impeding access to paper archives, staff will have to rely on the available electronic documents stored in the electronic filing applications such as ABAC etc. Arrangements for their accessibility from a back-up building are in place (Annex 10).

The measures implemented to ensure document accessibility are detailed further in Annex 5.

9. IT INFRASTRUCTURE AND SYSTEMS

The IT infrastructure and systems are critical for maintaining the activities of the ECSEL JU. The IT infrastructure and systems can suffer two types of disasters: a crash or unavailability of the servers and a crash or unavailability of the communication network. Annexes 4 and 5 describe the Disaster Recovery Plans for

the IT infrastructure and systems in case of complete or partial crash or unavailability of the JU servers located on the premises, somewhere else in Brussels or hosted outside of Brussels (EU infrastructure or not).

At this point in time, it is not envisioned to duplicate the IT infrastructure and systems. As shown in more detail in Annex 5, the recovery can be done with the measures already implemented: after a slight damage the recovery shall take place within a few hours or 1 to 2 days, while a severe damage may require a couple of weeks.

The JU's activity currently depends for part on an external server located in the Commission premises. This may imply that a crash or unavailability of the external communication network will block the access to the servers and stop parts of the activity in the JU. Discussions are ongoing to assess storage solutions in the cloud, including criteria on the security and confidentiality of data

10. FINANCIAL CIRCUITS

10.1. Set up of financial crisis circuits

In a crisis situation, the CMC may decide to use simplified financial circuits to make or delay payments.

The simplified financial circuits - based on the presumption that ABAC remains operational - require only a single initiating agent and an authorising officer (AO) complying with the "four eyes" principle of the Financial Regulations and rules. The key aspects of this simplified procedure is to open up access to budget lines much more freely to initiating agents and authorising officers assigned.

10.2. Electronic payments - ABAC/SAP/SWIFT are functioning:

In case the CMC decides to use the simplified management circuit, and ABAC/SAP/SWIFT are functioning, the following procedure shall apply:

The Executive Director or any other member of the CMC representing the Executive Director under the applicable deputising rules, will request to DG BUDG the activation of the crisis simplified financial circuit by means of completing and returning the attached form (see Annex 6).

The simplified financial circuits in ABAC, made available by DG BUDG, respect the "four eyes" principle as set out in Article 60.4 of the General Financial Regulation and require the use of:

- One initiator: this agent will perform operational and financial initiation;
- The visa of the AO who will perform the verification and the authorisation.

The AO has defined a list of staff to use this "crisis financial circuit" (Annex 7), which indicates the staff with the role of Initiating Agent and the role of Authorising Officer by sub-delegation. This list is coherent with the key staff members currently designated (one responsible person and two backups) for the financial functions (initiation and authorisation).

The use of this simplified financial circuit implies, therefore, that first and second level verification will temporally be suspended.

Subsequent audits of transactions performed during the crisis period will be feasible as the system keeps a specific audit trail of transactions executed under this special procedure.

The CMC will announce the end of the crisis and the Executive Director or any other member of the CMC representing the Director under the applicable deputising rules will inform DG BUDG to deactivate the crisis circuit by returning the same form as above (Annex 7).

This specific procedure covers the commitments, invoices/payments and recovery orders to be validated in ABAC WORKFLOW. (The ABAC ASSETS module will not be used during the crisis period).

With regard to financial management under H 2020 where the ownership of the systems and tools are kept in the Commission, a service level agreement shall be established.

10.3. Paper payments - ABAC/SAP/SWIFT are not functioning:

If ABAC, SAP or SWIFT is not functioning, the CMC will activate the paper procedure for the payments.

The latter procedure (sending letters to the bank) presents significant shortcomings and would require further prioritisation of payments. The procedure applies as follows:

1. The Authorising Officer sends by e-mail/brings a signed note to the Accounting Officer instructing him/her to pay:

- a given amount in EUR
- to a designated bank account, the bank account reference must include:
    a) bank account number
    b) name of the account holder and address (as deposited with the bank)c) IBAN number or if this is not available all required bank codes depending on the country (RIB, BLZ, Sorting).

2. The Accounting Officer will prepare a letter to the bank, using one of the templates (Annex 8 – Individual payments or Annex 9 – Mass payments) and will have it signed by authorised signatories (one of each "group", signatures laid down with the bank). The double signature requires that people having signatory power be present in one place either at the same time or subsequently to sign the letters. Letters will be sent either by registered post or by courier.

3. Once the situation is back to normal, the AO will need to regularise all these transactions in ABAC and via an exception report (as required by ICS 8). He may need to send to DG BUDG full supporting documents for new beneficiaries to definitely validate the Legal Entity/Bank Account, so as to allow for a correct posting in the accounts. The Accounting Officer will need to reconcile the transactions he/she introduced and sent, with the bank statements received from the relevant banks.

10.4. Payments of salaries in a crisis situation

If PMO cannot provide the files with the monthly calculations of the salaries and no payment delay is possible, the Accounting Officer will obtain from the bank a list with the data from the previous monthly payment of salaries to the staff. Based on this information, the AO will validate a mass payment using the electronic (see point 10.2) or paper procedure (see point 10.3). The paid amounts will be regularised with PMO in the next salary payment.

11. TRAINING & TESTING

Training and testing is essential for the effective development and operation of the BCP. Training sessions will be organized on a regular basis in collaboration with other JU's sharing the premises in TO 56 and for all staff including:

- Awareness training for all staff involved in crisis management (CMC)
- Training for CMC members
- Training for staff involved in critical functions.
- Training on reactiveness of BC Desk officer

The training will include a crisis simulation exercise. To be effective, testing will be repeated on a regular (annual) basis. The regular (at least) annual exercises will constitute a valuable input to be taken into consideration in the periodic updating/revision exercises of the BCP.

12. FINAL PROVISIONS

The BCP will be maintained and updated by the BC Desk Officer and reviewed at least once a year. Changes to the annexes and lists will be done on a regular basis, as necessary.

Change requests for the BCP document or its annexes will be mailed to the functional mailbox (ECSEL-BCP@ECSEL.europa.eu).

The BCP document will be available in the shared folder S:\5 MANAGEMENT and COORDINATION\5_03 Risk management. The global BCP document, including the annexes, will be kept in the file carried by the BC Desk officer and a copy notified to The Commission services involved (ARGUS and DG /HR-DS). An update of the contact details stored in the Duty Officer mobile telephone will be ensured by the BC Desk Officer.

13. ANNEXES

Note: Annexes are for restricted use only.

(1) Composition of the CMC

(2) Standard briefing agenda CMC – predictable crisis

(3) Standard briefing agenda CMC – sudden crisis

(4) Communication Plan (including 'cascade' staff list)

(5) ICT Disaster Recovery Plan – full procedure

(6) Note from DG BUDG on simplified financial circuits – D (2006) 11100 of 22/12/2006 + template to be used to send to DG BUDG to activate simplified circuit

(7) List of staff – crisis financial circuit

(8) Individual payments and mass payments template

(9) Mass payments template

(10) Support to the BCP from DG CNECT (mail dated 23.04.2015)

13.1. Annex 1 Composition of the CMC

Composition of the CMC
– updated at 05 May 2015

• Executive Director:	A. WILD
• Head of Administration	M. JEUNIAUX
• Head of Finance	J.P. CONTRERAS
• Head of Programmes:	Y. GIGASE
• DC Desk Officer:	HANANE EL FATMI
• Executive Assistant:	L. DE LESSINES
Optional:	
• Building manager ext.	A.BORGNIER (Knight Franck)
• Contact person in DG CNECT	0498. 98. 99. 00

13.2. Annex 2 Standard Briefing Agenda CMC

13.3. Annex 3 Standard Briefing Agenda CMC

Standard briefing agenda CMC

1. Presentation of situation by BCD Officer
2. Activation of BCP - code -
3. Immediate actions
4. Designation of the contact point
5. External services. Roles and resources
6. Communication to staff
7. Communication to stakeholders
8. Temporary office arrangements
9. Timing and actions list
10. Roles and tasks of CMC members
11. Next meeting(s)

Updated at 05 May 2015

13.4. Annex 4 Communication Plan

Communication Plan
- updated at 05 May 2015

Introduction

In the event of crisis, communication is to be targeted to the most important information, addressed to key actors (staff and stakeholders), with defining roles and channels within the JU.

1. Information of staff

Content and frequency of the communication to staff is designed by the CMC.

Staff members are to be informed immediately of the nature and consequences of the crisis with receiving instructions via the cascade list:

- HO Administration to all staff
- Channels to be used are telephone (mobile) and private e-mails.

2. Information to stakeholders

Based on available information at the CMC, the communication with stakeholders (Boards, partners ...) is conveyed by the Director's Office.

If applicable, a dedicated mail address is communicated to the stakeholders and accessible from the website and or CIRCA.

3. Contact lists

Contact lists are to be updated on a permanent basis. It will include the private details of staff and of actors involved in the recovery plan, as well as chair persons of Board and contact persons in the Commission services and with the Belgian authorities.

They are made available to all members of the CMC.

13.5. Annex 5 I.T. Business Continuity and Disaster Recovery

Business Continuity and Disaster Recovery (BC / DR)

- updated at 05 May 2015

I.T. as Part of BC / DR Planning

I.T. is an element which adds some risk from a BC or DR perspective but to a much greater extent it is an asset which can greatly assist both of those objectives.

The risk is obvious, because work activities are dependent on I.T. and information is archived in I.T. systems then the loss of those systems is a business risk.

With the limited resources available, the 6 JUs are already in a reasonably strong position regarding I.T. from a BC and DR perspective. Improvements are being implemented all the time and, with management approval, further improvements can be made. By far the biggest remaining issue from an I.T. perspective is a plan to mitigate a "burn-down" of the server room. This, along with other issues, is considered further in this document.

Measures taken to date to mitigate the risks

- All data on our servers is backed up daily and a weekly backup is taken off-site for archiving by a security company in case of a building "burn-down".
- In May 2011 a second connection to the outside world was installed (by Belgacom) to complement the existing cable installed in January 2011 (by COLT Telecommunications). Having 2 full capacity cables from different companies via different entry points in the building provides strong redundancy to this vital connection upon which ABAC, the FP7/H2020 Tools, e-mail and internet access depend.
- Laptop computers with VPN access are being deployed to more and more staff which lays the foundation for remote working possibilities in the event of no access to our premises.
- The architecture in the JU server room on the 5th floor was designed to eliminate single points of failure in so far as budgets would permit. For example, a 2nd firewall was purchased (900 Euro), a spare network switch (2,000 Euro). Moreover, the servers are virtualised across several physical machines any one of which can take over the functions of the other in the event of failure (with slightly reduced performance of course).
- We also have excess capacity in our cable network (450 cables for approx 130 staff of which 288 (48 x 6) can be active) and room in our server racks for emergency expansion.
- We have an Uninterrupted Power Supply (UPS) in our server room with a capacity of 30 minutes. Power failures are very rare and when they do happen they are usually

short "blips". Therefore, this UPS mitigates most of the risk by covering short outages and enabling a controlled shut-down for longer power failures.

- Most of our Application Systems and the data within them are hosted in European Commission data centres which are secured to very high standards. In the even of a "burn-down" of TO56, ABAC and the FP7/H2020 Tools will continue to function.
- For local files stored on desktops and laptops software is being installed that replicates automatically the data to the personal area of the user on the server. This is in turn captured by the server backups every day.

Server Room Replacement

If our server room on the 5th floor were to be rendered out-of-service due to a fire, flood or similar disaster then all 5 JU's would suffer loss of the following facilities:

- E-Mail (both local access and via webmail because the mail server is located in the server room)
- Access to the shared drive and any applications hosted on it
- Access to ABAC and the FP7/H2020 tools via s-Testa in our server room
- Access to internet
- Our telephone systems (because the PABX is in the server room)
- Needless to say, VPN access to all of the above would also cease.

If damage to the server room was slight, then replacement parts could be obtained and installed in a matter of hours or 1 or 2 days depending on the situation.

If, however, our building was seriously damaged by fire, flooding, structural damage or other problems then a complete replacement of our server room would be necessary. That could take a couple of weeks or more.

At this point in time, no satisfactory solution has been identified to accelerate the recovery after a serious damage. This point shall be improved in the future version of the DRP.

S-Testa

One of the facilities in our server room is the often mentioned s-Testa rack. It requires particular consideration here.

S-Testa is a very special piece of hardware installed by Orange. It is an encryption and secure communication system and the only approved way to connect to ABAC and other sensitive applications provided by the European Commission.

It is a sealed unit and neither the JU's nor Real Dolmen can access it. We cannot back it up, replicate it, virtualise it or re-install it on a server farm. This can only be done by Orange.

Measures have been taken to ensure an alternative access to ABAC and the FP7 tools by the ECSEL JU staff using EC workstations.

Other Aspects

It is worth mentioning that most, if not all, of the JTI web sites are hosted on external facilities so any problem with our servers facilities will have no effect on our web sites or extranets (e.g. CIRCA which is used by at least 2 JTIs). This is very important because we can communicate the impact of any problems via our web sites and announce work-around solutions, alternative contact information, re-scheduling of meetings etc.

The extranet is similarly independent of the infrastructure at TO56 and can be a useful tool when disaster strikes. This diversity of systems and the hosting of systems is a deliberate part of our I.T. strategy.

Another aspect of communications which needs to be considered is telephony. Mobile phones have been provided for key employees to be used in the event of a disaster.

13.6. Annex 6 Simplified Financial Circuits

Simplified financial circuits and relations with the Commission services DG BUDG

FORM TO BE COMPLETED IN ORDER TO HAVE CRISIS FINANCIAL CIRCUIT ACTIVATED OR DEACTIVATED

Form	**ABAC Crisis Management - (De-)Activation**		
Document Date	***Reg. Nr (ARES Number to be given by DG BUDG)***	***Start Date***	***End Date*** *{optional}*

In conformity to the procedure "ABAC Security Measures in case of a major Crisis",

I, _____ *{full name}*, hereby request the activation/de-activation of the crisis-settings for DG/Service _____ *{organisation}* according to the dates mentioned above.

Please introduce into ABAC the following modalities: *{Tick appropriate box and/or complete}*

☐	The crisis-workflow domain is to be used exclusively **OR**
☐	The crisis-workflow domain is to be opened in addition to the standard settings
☐	The crisis-workflow domain must be accessible to **all** staff currently having the role of Initiating Agent. **OR**
☐	The crisis-workflow domain must be accessible **exclusively** to following list of the staff with the role of Initiating Agent.:
	• ....
☐	The crisis-workflow domain must be accessible to **all** staff currently having the role of Authorising Officer by (Sub-)delegation
☐	The crisis-workflow domain must be accessible **exclusively** to following list of the staff with the role of Authorising Officer by (Sub-)delegation:
	• ...

_____ *{Signature and Title}*

To be sent either by fax or by e-mail (scan or PDF) to BUDG MPM TEAM and BUDG USM ABAC WF– Fax: 02/299.16.54

13.7. Annex 7 Crisis Financial Circuit

Crisis Financial Circuit: Simplified workflows and off budget payments

---

Financial actors (updated at 05 May 2015)

DUTIES	STAFF MEMBER	BACK UP
Initiation	A. Varvaroussis	E. Bamparoutsi
Verification and authorisation	A. Wild	M. Jeuniaux
Accounting	J.P. Contreras	S. San Jose Fernandez

13.8. Annex 8 Template for individual and mass payments

13.9. Annex 9 Appendix for mass payments

Template for Individual and Mass Payments

Brussels,
Ref./

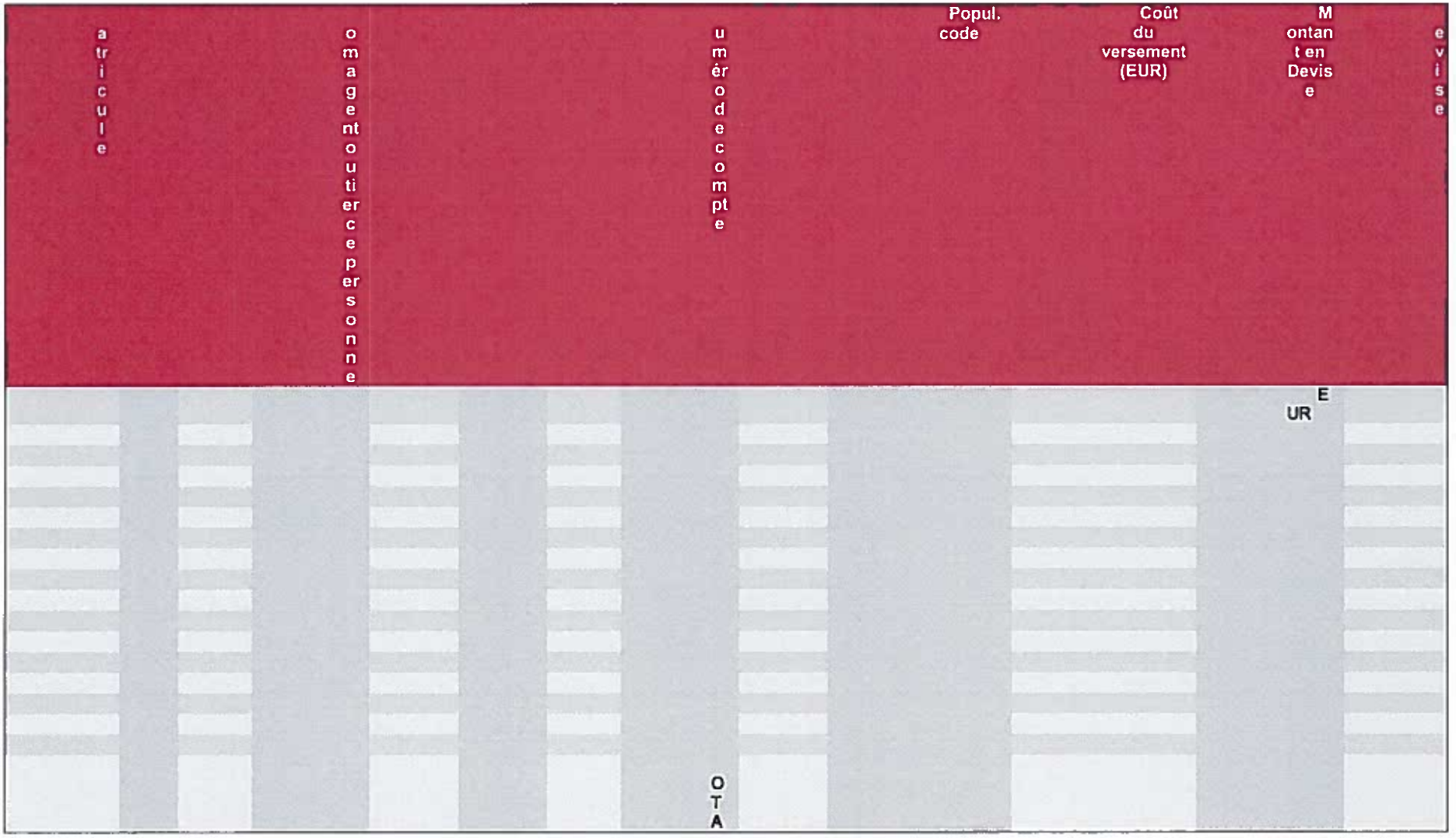
Note for the attention of (ECSEL JU Bank name)
Subject: Payment according to Art. 10.3 of ECSEL JU BCP - Simplified Financial Circuit

Dear Sir,
According to Article 10.3 of ECSEL JU Business Continuity Plan concerning the activation of the simplified financial circuit,
Please pay,

Best Regards,
Signed by ECSEL JU Accounting Officer

Enclosed:
Template to be annexed for mass payments (below).

Appendix: Template to be used in case of mass payments.




L

13.10.Annex 10 EC commitment to support the ECSEL JU BC/DR Plan

Support of the Services of the Commission –DG CNECT

Commitment to the participation to the BCP of ECSEL JU

Location at BU 25 2/120

Ref. Ares(2015)1721912 - 23/04/2015

DG CNECT /A4/MH/jg

NOTE FOR THE ATTENTION OF ANDREAS WILD, EXECUTIVE DIRECTOR ECSEL JU

Subject: Commission support to ECSEL JU Business Continuity and Disaster Recovery Plans

Dear Andreas,

Further to your request for support by the Commission in case of crisis or disaster in the ECSEL JU's premises, I confirm that DG CONNECT will provide the following services upon request:

- ***The allocation of a space equipped with four workstations in BU25 2nd floor;***
- ***The creation of two functional accounts CNECT-BCP-ECSEL and CNECT-DRP-ECSEL;***
- ***The creation of two LDAP accounts for accessing the internet.***

The passwords will be provided by DG CONNECT IRM upon request by the ECSEL JU. If Business Continuity is activated (at Commission level or at local level by the Executive Director of the ECSEL JU), according to their business continuity plans, the JU will directly contact DG CONNECT via the CNECT Duty Officer (0498 98 99 00 / 0498 98 99 01). The facilities will be available within one working day. Tests should be announced twelve working days in advance.

Yours sincerely,

[e-Signed] Khalil Rouhana