Twinview
Platform Security Compliance

September 2022 – Rev C

Twinview®

Twinview Compliance

OVERVIEW

We take your data seriously and our cloud products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations of compliance, or audit reports against standards globally.

This document highlights at a high level our security measures and how we keep your data safe. This document will not go into detail of the architecture or infrastructure of the platform in detail as this would go against our policy of protection by obscurity. Such information is available on request to our partners, affiliates and included in individual SLA's or on request to those with an NDA in place.

DATA STORAGE AND HOSTING

By default, in your data is hosted on the Amazon AWS infrastructure on which Twinview is hosted. The Twinview application uses the AWS eu-west-2 region (London). Client specific project data can be stored in the local AWS region set at a project level, based on the project's location defined in Twinview.

Twinview can also be hosted in another cloud provider such as Microsoft Azure, Goggle Cloud or the clients own cloud provider. These deployments are 'special case' and security policy's and compliance will be established and detailed as part of the SLA agreement between the client and Twinview.

ISO/IEC 27001:2013 COMPLIANCE

Twinview is currently undergoing its certification to achieve ISO27001 :2013 compliance, and we hope to have official certification in-place by January 2023.

CYBER ESSENTIALLS+ COMPLIANCE

Cyber security is not just about our cloud based product Twinview, it is equally as important to protect you data and information that we hold at our physical locations and offices. Twinview and its parent company, have achieved Cyber Essentials Plus certification. A copy of this certificate is included in Appendix D.

SERVICE LEVEL AGREEMENTS

Twinview has a standard starting SLA we use with clients, however this will vary depending upon hosting infrastructure chosen and client specific requirements and needs. We typically agree a client specific SLA for our Affiliate and Enterprise customers.

Because we utilise the Amazon AWS infrastructure, any SLA we provide would be in addition to the standard AWS SLA's which are available here for the services we use on AWS:

S3 SLA
https://aws.amazon.com/s3/sla/

Route 53 SLA
https://aws.amazon.com/route53/sla/

EC2 SLA
https://aws.amazon.com/compute/sla/

Amazon RDS
https://aws.amazon.com/rds/sla/

PRODUCT UPDATES AND PATCHING

Twinview typically has an ongoing roadmap for development for 2 years, with development pipeline locked in at 6 months. We consult with our customers, and resellers to understand requirements, features, and priorities.

Our separate internal Dev Ops team, ensure the platform remains stable and secure and they sit outside of the main development team.

CHANGE MANAGEMENT PROCESSES

Being a dynamic and evolving platform, we employ an Adaptive Change management process, small, gradual, iterative changes to evolve our platform, processes, workflows, and strategies.

Where Transformational changes are required, these are carried out over a longer timeframe of 6 months, and follow a 5-step process, that includes a documented Strategic planning, Implementation and Analysing of Results.

DATA CENTRE PHYSICAL SECURITY

Our standard hosting utilises Amazon AWS. You can read here about how amazon complies and exceeds industry standards regarding both cyber and physical security:

https://aws.amazon.com/compliance/data-center/controls/

OFFICE & PHYSICAL SECURITY

Our offices are monitored 24/7 by CCTV and are alarmed outside normal hours of operation with the alarm system linked to the local police and fire service. The building is segmented into security zones, with access control required between each zone.

We have documented processes for all visitors to premises, which includes a sign-in process. Guests have limited access to the building, physical resources, and a separate network infrastructure.

The building is protected by an approved fire alarm system, which is directly connected to the fire department.

1. Burglar Alarm System with Redcare, a log of operations is retained within the system key-panel
2. Fire Alarm System with Redcare, a log of operations is retained within the system key-panel.
3. Door Access System, a log of entries/exits is downloaded and manually recorded in a Spreadsheet.
4. Visitor Log iPad Application, a log of visits is retained within the App.
5. Receptionist to meet and direct visitors.
6. External CCTV.

Data is retained for the following systems:

CCTV System – 28 days.
Door Access System– 28 days.
Visitor Logs – 28 days.

COMPANY EMPLOYEE BACKGROUND CHECKS

All Twinview employees undergo a standard background check from previous employers as well as Passport and DBS check.

COMPANY EMPLOYE POLICIES

All personnel policies are contained in our BMS (Business Management System) document which contains all business policies and employees agree to adopt these policies as part of their employment. A copy of this can be provided on Request.

USE OF CUSTOMER DATA IN TESTING/DEVELOPMENT ENVIROMENT

We have a dedicated sandbox and staging environment development, testing, and demonstration purposes (https://staging.twinview.com & https://demo.twinview.com).

These are separate environments, with separate hosting and contain no sensitive client data (apart from pre-approved non sensitive demo projects in relation to staging).

Twinview will always consult with the client before using their data for development or testing in the staging or demo environment.

BACKUP AND DATA RETENTION

Backups are undertaken regularly, and we employ the grandfather-Father-Son backup strategy. Platform Daily Backups are kept for 30 days and are held on a dedicated backup server, this can be amended on a client-by-client basis if required by utilizing a dedicated server (on premise or cloud).

Backups containing customer data is 30 Days, in accordance with legal obligations and ICO advice. This however can be amended on a client-by-client basis and agreed in the Terms and SLA.

Company's internal business servers are backed up every night, with weekly tape backups to a secure off-site location – See Appendix C.

The BCP IT plan is tested and assessed every 12 months as defined in Appendix B

INCIDENT RESPONSE

Twinview has a documented incident response process in place. This documents the processes in place if a major Incident occurs.

This document is included in Appendix A

USEFUL CONTACTS:

If you need further information or would like to discuss any of the above in more detail, please contact:

PRODUCT MANAGER & DEVELOPER LEAD
Adam Ward
adam.ward@twinview.com

DATA SECURITY OFFICER
Andrew Parker
Andrew.parker@spacegroup.com

APPENDIX A - Information Security Incident Response Procedure

Twinview®

Information Security Incident Response Procedure

Document Ref.	**GDPR-DOC-15**
Version:	**1**
Dated:	**08 February 2018**
Document Author:	**Andrew Parker**
Document Owner:	**Andrew Parker**

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title
Rob Charlton	CEO

Approval

Name	Position	Signature	Date
Rob Charlton	CEO		

Contents

List of Figures

List of Tables

1 Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of Twinview Ltd, including those potentially affecting personal data for which the organization is a controller. It is intended to ensure a quick, effective and orderly response to an information security breach.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- provide a concise overview of how Twinview Ltd will respond to an incident
- set out who will respond to an incident and their roles and responsibilities
- describe the facilities that are in place to help with the management of the incident
- define how decisions will be taken with regard to our response to an incident
- explain how communication within the organization and with external parties will be handled
- provide contact details for key people and external agencies
- define what will happen once the incident is resolved and the responders are stood down

All members of staff named in this document will be given a copy which they must have available when required.

Contact details will be checked and updated at least two times a year. Changes to contact or other relevant details that occur outside of these scheduled checks should be sent to security@spacegroup.co.uk as soon as possible after the change has occurred.

All personal information collected as part of the incident response procedure and contained in this document will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

2 Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.

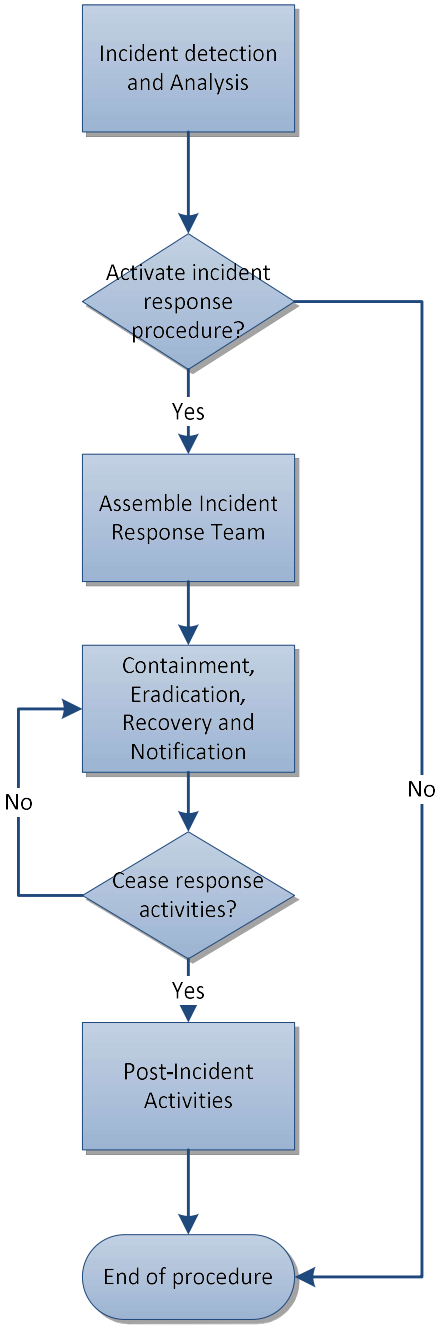

Figure 1 – Incident response flowchart

These steps are explained in more detail in the rest of this procedure.

3 Incident Detection and Analysis

An incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within Twinview Ltd or by employees noticing unusual activity (see the *Information Security Event Assessment Procedure* for details of how events are assessed). Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of a proactive approach to information security is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets (including personal data) that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact to them
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data), business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

As a result of this initial analysis, any member of the management team has the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Incident Response Procedure should be activated.

4 Activating the Incident Response Procedure

Once notified of an incident the Team Leader must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of the Incident Response Team (IRT).

Guidelines for whether a formal incident response should be initiated for any particular incident of which the Team Leader has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information, including personal data
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organization

In the event of disagreement or uncertainty about whether or not to activate an incident response the decision of the Team Leader will be final.

If it is decided not to activate the procedure then a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

5 Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that all role holders (or their deputies if main role holders are un-contactable) are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location.

The exception is the Incident Liaison who will be asked to attend the location of the incident (if different) in order to start to gather information for the incident assessment that the IRT will conduct so that an appropriate response can be determined.

5.1 Incident Response Team Members

The Incident Response Team will generally consist of the following people in the roles specified and with the stated deputies, although the exact make-up of the team will vary according to the nature of the incident.

Role/Business Area	Main role holder	Deputy
Team Leader	Rob Charlton	
Team Facilitator	Lynn Telford	
Incident Liaison	Andrew Parker	
Information Technology	Andrew Parker	
Business Operations	Rob Charlton	
Facilities Management	Diane Charlton	
Health and Safety	Lynn Telford	
Human Resources	Diane Charlton	
Business Continuity Planning	Andrew Parker	
Communications (PR and Media Relations)	Rob Charlton	
Legal and Regulatory	Diane Charlton	

Table 1 – Incident response team members

Contact details for the above are listed at Appendix A of this document.

5.2 Roles and Responsibilities

The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides whether or not to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement

Team Facilitator

- Supports the incident response team
- Co-ordinates resources within the command centre
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command centre
- Facilitates communication via email, fax, telephone or other methods
- Monitors external information feeds such as news

Incident Liaison

- Attends the site of the incident as quickly as possible
- Assesses the extent and impact of the incident
- Provides first-person account of the situation to the IRT
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT

Information Technology

- Provides input on technology-related issues
- Assists with impact assessment

Business Operations

- Contributes to decision-making based on knowledge of business operations, products and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization

Facilities Management

- Deals with aspects of physical security and access
- Provides security presence if required

Health and Safety

- Assesses the risk to life and limb of the incident
- Ensures that legal responsibilities for health and safety are met at all times
- Liaises with emergency services such as police, fire and medical
- Considers environmental issues with respect to the incident

Human Resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organization employees
- Advises on capability and disciplinary issues

Business Continuity Planning

- Provide advice on business continuity options
- Invoke business continuity plans if required

Communications (PR and Media Relations)

- Responsible for ensuring internal communications are effective
- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g. customers, shareholders

Legal and Regulatory

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks
- Assesses the actual and potential legal implications of the incident and subsequent actions

5.3 Incident Management, Monitoring and Communication

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. A standard agenda for these meeting is at Appendix C. The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minuted by the Team Facilitator.

The Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be co-ordinated with the IRT meetings so that the latest information is available for each meeting.

5.4 Communication Procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, both landline and mobile. Email should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
  - Ask if the contact is available elsewhere
  - If they cannot be contacted leave a message to contact you on a given number
  - Do not provide details of the Incident
- Always document call time details, responses and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action at a later date.

5.4.1 Communication to the Data Protection Supervisory Authority

It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. The Twinview Ltd *Personal Data Breach Notification Procedure* must be used for this purpose. In the event that the 72-hour target is not met, reasons for the delay must be given.

Contact details for the data protection supervisory authority are listed in Appendix B.

5.4.2 Communication with Personal Data Subjects

Where an incident affects personal data, a decision must be taken by the IRT regarding the extent, timing and content of communication with data subjects. The EU GDPR requires that communication must happen “without undue delay” if the breach is likely to result in “a high risk to the rights and freedoms of natural persons”. The Twinview Ltd *Personal Data Breach Notification Procedure* must be used for this purpose.

5.4.3 Other External Communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Shareholders
- Regulatory bodies

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them. A list of some external agencies is given at Appendix B.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

5.4.4 Communication with the Media

In general the communication strategy with respect to the media will be to issue updates via top management. No members of staff should give an interview with the media unless this is pre-authorised by the IRT.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media the following guidelines should be observed:

- Personal information should be protected at all times
- Stick to the facts and do not speculate about the incident or its cause
- Ensure legal advice is obtained prior to any statements being issued
- Try to pre-empt questions that may reasonably be asked
- Emphasise that a prepared response has been activated and that everything possible is being done

The following members of staff will be appointed spokespeople for the organization if further information is to be issued e.g. at a press conference:

Name	Role	Incident Scale
Rob Charlton	CEO	Low
Rob Charlton	CEO	Medium
Rob Charlton	CEO	High

Table 2 - Media spokespeople

The most appropriate spokesperson will depend upon the scale of the incident and its effect on customers, supplier, the public and other stakeholders.

6 Incident Containment, Eradication, Recovery and Notification

6.1 Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g. by waking up a laptop. It is recommended that specialist advice should be obtained at this point – see contacts at Appendix B.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g. time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.

Principle 4 – The person in charge must ensure that the guidelines are followed.

Prior to the arrival of a specialist basic information should be collected.

This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident
- Original documents, including records of who found them, where and when
- Details of any witnesses

Once collected, the evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

6.2 Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

6.3 Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

6.4 Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

Twinview Ltd will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and Twinview Ltd will cooperate in full with such proceedings.

7 Post-Incident Activity

The Team Leader will decide, based on the latest information from the Incident Liaison and other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule
- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Team Leader should define the next actions to be taken. These may include:

- Less frequent meetings of the IRT e.g. weekly depending on the circumstances
- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff not involved in further work to return to normal duties

All actions taken as part of standing down should be recorded.

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.

8 APPENDIX A – Initial Response Contact Sheet

The following table should be used to record successful and unsuccessful initial contact with members of the IRT:

Name	Role in Plan	Office Number	Home Number	Mobile Number	Date/Time	Outcome (Contacted / No Answer / Message Left / Unreachable)	ETA (if contacted)
Rob Charlton	Team Leader / Business Operations / Communications (PR and Media Relations)	0191 2236600		Redacted			
Lynn Telford	Team Facilitator / Health and Safety	0191 2236600		Redacted			
Andrew Parker	Incident Liaison / Information Technology / Business Continuity Planning	0191 2236600		Redacted			
Diane	Facilities Management	0191		Redacted			

Name	Role in Plan	Office Number	Home Number	Mobile Number	Date/Time	Outcome (Contacted / No Answer / Message Left / Unreachable)	ETA (if contacted)
Charlton	/ Human Resources / Legal and Regulatory	2236600					

9 APPENDIX B – Useful External Contacts

The following table shows the contact details of third parties who may be useful depending on the nature of the incident:

Organization	Contact	Telephone Number	Email
Data Protection Supervisory Authority	Information Commissioner's Office	0303 123 1113	
Law Enforcement Agency	Northumbria Police	0191 214 6555	
Internet Service Provider	ITPS	0191 442 0250	Itps.support@itps.co.uk
Industry Association	RIBA	020 7580 5533	
Industry Regulator	ARB	020 7580 5861	

10 APPENDIX C - Standard Incident Response Team Meeting Agenda

It is recommended that the following standard agenda be used for meetings of the Incident Response Team.

AGENDA

Attendees: All members of Incident Response Team

Location: Spaceworks, or ITPS Recovery Centre if Spaceworks is unavailable.

Frequency: Every 1 Day

Chair: Team Leader

Minutes: Team Facilitator

1. Actions from previous meeting
2. Incident status update
3. Decisions required
4. Task allocation
5. Internal communications
6. External communications
7. Standing down
8. Any other business

APPENDIX B - D6.1 - Data Protection Procedure

Ref D6.1	Data Protection	Twinview®
Primary ID: BMS D6.1	Issue/Revision No: 05	Supersedes No: 04
Approval: Rob Charlton (CEO)	Author: Andrew Parker – IT Manager	

1.00 Purpose

1.1 To maintain and protect company information

2.0 User Account Security

2.1 The company maintains a password for every user account to ensure Data Security, Privacy and Auditing. You must not disclose your password to anyone else apart form the following parties who may ask for it to enable them to carry out their business.

- IT
- Your Group Leader
- Director

2.2 Password Reset to allow Access to a colleague's account

2.2.1 Should you require access to a colleagues account e.g. to access their email, you must obtain the permission of their Group Leader. The Group Leader must communicate this to IT, if the Group Leader is unavailable you can obtain permission from their Business Unit Leader or HR. Items required by IT are:

- Account with needs to be accessed
- Reason
- Employee's requiring access

Using the information supplied, IT will confirm (by email) to the following people access has been granted:

- The Employee who's account is being accessed
- The Employee who needs access
- Group Leader
- Talent Department

2.3 Password Change Procedure

2.3.1 All employees are required to change their password every 90 days. When logging onto your PC, if you are prompted to change your password you must ensure it conforms to the following set of requirements:

Your password should:

- Be at least 7 characters
- Contain at least one number
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Not contain your first or last name
- Not be a password you have used in the last 12 months.

An example password that meets the requirements: Passw0rd

2.4 Password Unlock Procedure

2.4.1 You are allowed 5 unsuccessful login attempts before the system locks your account. To unlock your account contact the IT Helpdesk on extension 6616 or 6653 for a Password Reset
If you have forgotten your password, IT will set your password to a random password and communicate this to you.
The next time you login, you will be prompted to create a new password (see Password Change Procedure)

2.5 New User Account Password Procedure

2.5.1 When accounts are created for new employees, IT will generate a random password so that existing employees cannot guess the password of the new employees account.

3.00 Data Recovery

3.1 Backup Procedure

3.1.1 Newcastle – Every weekday all servers are incrementally backed up to a Backup Server (also located at Spaceworks) using the Veeam backup application. Veeam maintains a full backup of every Newcastle server, incremental backups are injected into the full backup to keep the full backup up to date. Every weekend the full Veeam backup is also written to LTO tape, and each weekday the incremental Veeam backup is written to LTO tape.
Weekday tapes and the most recent weekend tapes are stored off site with the IT Manager or delegated person. Older weekend tapes are stored at Spaceworks in a fire rated safe.
Full tape rotation is achieved after three months.

Additionally every weekday, all Newcastle servers are replicated to the Disaster Recovery Server (using Veeam) located in Birtley at ITPS's Datacentre.

Each Veeam backup is checked for errors each weekend, a log of the backup is saved to the server. Each tape backup is verified immediately after the backup has completed, a log of the backup is saved to the server and to the tape backup itself.

3.2 Backup Test Restore Procedure

3.2.1 Once per week a Veeam test restore is performed to ensure we can restore files from the Veeam backup located on the Backup Server. Once per quarter a test restore is run to ensure we can restore files from at least one of the tapes before the cycle restarts.

3.3 Software Storage Procedure

3.3.1 All client software is zipped and copied to a repository on the server, and is additionally held on a USB drive by the IT Manager. Software is filed by Author/Manufacturer and any Product / License Keys are included within the zip file

3.4 Hardware Disposal Procedure

3.4.1 All Hardware is disposed using a nominated Hardware Disposal company. Any Hardware which contains data is cleansed before it is resold or donated to other organisations/individuals.

APPENDIX C - Business Continuity Plan

Ref D6.12	Business Continuity Plan	Twinview
Primary ID: BMS D6.	D6 _ 12	Supersedes No: 11
Approval: Rob Charlton (CEO)	Author: Andrew Parker – Approval: Rob Charlton (CEO)	

1.0 INTENT

To maintain the security of the company's data and have access to premises which will allow the company to trade after a major disruption.

2.0 Table of Contents

3.0 Business Continuity Team Members

- Chief Executive Officer
- Group Operational Manager
- Information Technology Leader
- Applications Manager
- Financial Accountant

If it is not possible to meet at the business premises, an initial meeting will take place at the Regus Centre, Newcastle Quayside:

Regus Centre,
Rotterdam house
116 Quayside
Newcastle upon Tyne
NE1 3DY
Tel: 0191 2064000

Key actions that need to be performed before the first meeting is convened:

1. All team members should be notified an event has occurred
2. One team member should be given the task of visiting the site to:
   a. Assess if a meeting can take place at the company premises or not.
   b. Produce a Situation Report summarising the problems facing the team.
3. Should the team require an offsite meeting space, one team member should be given the task of arranging the meeting room and communicating the timings to the other team members.

Refer to Appendix 1 for each team members contact details.

4.0 Threats to Business Continuity

Threats to Business Continuity can be defined into the following categories:

- Partial loss of premises due to destruction. (Fire, flood, burglary, storm, terrorism)
- Total loss of premises due to destruction (Fire, flood, burglary, storm, terrorism)
- Partial loss of premises due to access restrictions (problem with neighbouring properties such as dilapidation, biological threat, hazardous threat).
- Total loss of premises due to access restrictions (problem with neighbouring properties such as dilapidation, biological threat, hazardous threat.
- Partial loss of electronic data (mechanical failure, electronic failure, virus outbreak, hacking).
- Total loss of electronic data (mechanical failure, electronic failure, virus outbreak, hacking).
- Temporary loss of utilities (Water, Electricity, Gas, Internet)
- Temporary or permanent loss of labour (Epidemic, illness, strike)

5.0 Premises

5.1 Insurance

The Financial Accountant is responsible for premises insurance; the company maintains the following insurance policies to ensure it is covered in the event of a claim.

The company hold Business Interruption Insurance in addition to contents insurance.

Sums incurred are:

- Loss of rent receivable - £105,000
- Loss of income and increased cost of working - £250,000
- Additional increased cost of working - £250,000
- The applicable indemnity period is 12 months

The Financial Accountant will ensure that all the requirements of the company contained within the insurance policy are adhered to.

5.2 Premises Security

Spaceworks

The Group Operational Manager is responsible for premises security at Spaceworks, the company maintains the following systems to minimise the risk of burglary.

a) BS Standard door locks
b) BS Standard alarm system covering all perimeter access with Redcare GSM link to a central monitoring agency.

The Group Operational Manager will ensure these systems are operating every day, reporting faults to suppliers when systems fail.

The Group Operational manager is also responsible for ensuring any service or maintenance contracts are invoiced and paid in accordance with the supplier's terms and conditions.

5.3 Premises Repairs

Spaceworks

The Group Operational Manager is responsible for ensuring that all of the repairs to Spaceworks are carried out by an approved company and that the quality of the work is of a good standard.

Where a standard of repair is required by the insurance policy, those repairs should be carried out to that standard or negotiated with the insurance company.

See Appendix 1 for a list of all suppliers.

5.4 Relocation

Spaceworks

If due to an event, some or all staff are required to be relocated to separate premises, those premises have been identified ahead of time, the business will relocate to ITPS;s Recovery Centre.

When an event occurs which requires the relocation of some or all of the staff, ITPS should be contacted to invoke the contract and make the office space available.

See Appendix 1 for contact details.

Services which will be provided by ITPS, as follows:

- Desks
- PC's
- Telephones
- Local area network cabling
- Internet connection, 10Mbit/sec, 1:1 contention and static IP address
- Rack space

Additional equipment not supplied will need to be catered for on a separate basis:

- Networked photocopiers / printers / fax
- Servers
- Plotters

6.0 IT

6.1 Data Security

The IT Leader is required to maintain a tape backup system to ensure all electronic data is backed up on a daily basis (except for weekends). The most recent Friday tapes are stored off site with the IT Manager. All other tapes are stored on site in a fire rated safe. Additionally all data is replicated to ITPS's Recovery Centre each evening.
Friday – 1
Friday – 2
Friday – 3
Friday – 4
Friday – 5
Friday – 6
Friday – 7
Friday – 8
Friday – 9
Friday – 10
Friday – 11
Friday – 12
All incremental daily backups (Mon-Thurs) are copied to the IT Managers laptop each day.

The rest of the tapes are held in a fire resistant safe located within the office, safe keys are held by the IT Leader and Finance.

Once a month a tape is tested to ensure it can restore a set of files.

6.2 Password Repository

A list of passwords is kept on the Dropbox and can be accessed anywhere there is an internet connection and web browser.

The IT Manager, Applications Manager and Finance all have login credentials for Dropbox.

6.3 Server Replacement

Each server has a Maintenance Agreement covering the hardware for any failed parts.

The IT Asset Registers (Held on Dropbox) hold details of the server serial numbers.

ITPS (see Appendix 1) will manage the repair procedure, they will require the server serial number when a support call is logged with them.

The server maintenance agreements will not cover servers in the case of damage not due to a failed part e.g. fire, in this event the company will need to purchase a server(s) to replace the damaged equipment and reclaim the cost via insurance.

In the event of a disaster to the Spaceworks premises where the staff recover to the ITPS Recovery Centre, an existing backup server (located at the Recover Centre) will be made available and configured to allow access to the data for staff who are operating from the Recover Centre or from VPN. The backup server has a complete replicated copy of all the data in Newcastle, the data being at most one (working) day old.

6.4 PC Replacement

Each PC has a standard maintenance agreement which spans from 1 year.

Contacting HP Technical Support will ascertain if the failed PC is under warranty, should it not be the IT Department will attempt a repair, if this fails a replacement PC will be supplied to the employee.

In the event of a disaster to the Spaceworks premises where the staff recover to the ITPS Recovery Centre, if required a PC will be made available in the short-term whilst replacement machines are ordered, delivered and configured.

6.5 Internet Connection

The internet connections at Spaceworks are provided on a leased line with a premier service level agreement.

If the internet connection fails at Spaceworks contact ITPS (see Appendix 1) to report a fault.

If the business needs to relocate to the Recover Centre, ITPS will provide an internet connection with 100Mbit/sec 1:1 contention ratio and static IP address.

6.6 Photocopiers

All photocopiers are backed by a Service Level Agreement which is included in the cost of running the photocopier.

Should any photocopier need repair, the support number is located in the copier itself. (Details also in Appendix 1).

The photocopier SLA does not protect it from faults due to damage eg fire. In this event a new photocopier would need to be purchased should a repair not be feasible.

6.7 Plotters

Space operates two inkjet plotters to provide A0, A1 and A2 printing facilities (A3 and A4 sizes are provided by the Konica Bizhub Photocopiers). Both machines can print A1 and A2, A1 being the most common size for printing, one machine can print A0.

No HP plotter has a maintenance agreement, the company pays for repairs based on a time and materials basis, this is due to the unlikely occurrence of both machines being unserviceable at the same time.

In the event of a failure due to fire or hardware failure, where both plotters are permanently unserviceable, initially employees will be expected to use reprographics whilst a suitable replacement can be sourced from Standing Stone (see appendix 1 for contact details).

6.8 Cameras

Any camera which is faulty and beyond repair can be renewed by using one of the Mail Order IT Suppliers (see Appendix 1 for contact details).

6.9 Scanners

Any scanner which is faulty and beyond repair can be renewed by using one of the Mail Order IT suppliers (see Appendix 1 for contact details).

7.0 Telecommunications

7.1 PBX

The company's telephony and facsimile systems do have maintenance agreements to ensure equipment is repaired in the event of a fault. There is however no cover for the failure of a system due to a damage event except replacement from an insurance claim.

If the business recovers to ITPS's Recovery Centre, a telephone will be available for each member of staff located there.

7.2 Call Diversion

Should the PBX or phone lines become damaged or become faulty, TSG should be contacted and asked to divert incoming calls to a mobile phone initially. If the company is recovering to the Recovery Centre, then the calls can be diverted there once the recovery has been completed.

Messages are taken on behalf of the employee, the employee can then return the call from another mobile phone.

Messages can then be relayed to the employee by one of the following methods (if available):

- Message pad
- Internal voicemail
- Internal email
- Fax

In the event of a Disaster Recover Invocation, at a cost to Space, TSG can implement a service whereby the company can choose where each single DDI is diverted to, this is a premium service as opposed to the block redirection of all the DDI's to a single number (which will not be charged for). This will be useful to take care of the tenants who will lose the ability to receive calls and will eb relying on Space to handle their calls on their behalf whilst not working in the same location (as there is no provision to provide Disaster Recovery seats for the tenants).

8.0 Physical Documents

8.1 There is no provision for recovering physical documents which have been destroyed.

9. Mail Diversion

9.1 In the event of premises re-location, the Royal Mail must be instructed to deliver post to an alternative location.

The Group Operational Manager will be tasked with setting up a PO Box for the company's incoming mail and will also instruct Royal Mail of new address(s).

A member of staff must be tasked with collecting the mail, sorting and then distributing.

10. Staff Communications

10.1 The Group Operational Manager will be tasked with ensuring all employees are kept informed about the progress of recovery.

10.2 The Group Operational Manager is required to keep an up to date list of employee contact details (see Appendix 1).

10.3 Together with the other team members the Group Operation manager will compose a daily situation report which will be communicated to all employees each working day, items included in the communication include:

- Premises repair / relocation
- IT systems restoration
- Each project's status e.g. on hold, progressing slowly, progressing normally.
- Staff availability e.g. on holiday, sick, available
- Payroll processing
- Message from the Chief Executive Officer

Items 1, 2 and 3 will include estimates about when these processes are to be completed.

10.4 Methods of communication will be dependent on how each employee can receive notifications, but these can include:

- Email
- Telephone call
- Text message
- Website posting
- Letter

The first communication should be by letter, within the letter employees should be asked to notify the Talent Leader if there contact details are correct. Subsequent communication can be done by any other method.

11.0 Client Communication

11.1 The Chief Executive will be tasked with ensuring all affected clients are kept informed about the progress of recovery.

The IT Leader is required to keep an up to date list of client contact details, exported from the company intranet (see Appendix 1).

Together with the other team members the Chief Executive Officer will compose a letter which will be communicated to all affected Clients, items included in the communication to include:

- Premises repair / relocation
- IT systems restoration
- Their project's status
- Message from the Chief Executive Officer

Items 1,2 & 3 will include estimates about when these processes are to be completed.

12.0 Finance

12.1 Payroll

In order to ensure employees are paid according to their employment contract's terms and conditions, Finance will ensure they have an offsite copy of all salary details (and bank account numbers) so that the correct payments can be made in a timely fashion.

12.2 Alternative methods of payment

In order to process the payroll, finance may need to make payments to employees without using the usual BACS processing system.

Alternative methods include:

- Internet banking
- Over the counter payments to a Bank Teller
- Cheque mailed to home address.

Internet banking will need to be set up before any problems occur and a cheque book will need to be stored off site to ensure that they are available.

13 Emergency overdraft facility

13.1 Some suppliers may require payment up front for equipment if they learn the company is suffering problems and it may take some time for insurance monies to be paid due to the claims process.
For example: 100 PC's will require approximately £70,000 credit.

Negotiating an emergency overdraft facility (to be evoked when an event occurs) with the bank ahead of time would ensure equipment could be paid for should this be necessary.

Appendix 1

Contact Details

Name	Position	Contact
Andrew Parker	Information Technology Leader	
Sean Hood	Applications Manager	
Neil McGlew	Financial Accountant	
Diane Charlton	Group Operational Manager	
Rob Charlton	Chief Executive	

Staff Contact Details

To obtain the staff contact details log in to the Dropbox Business Continuity Account using your login credentials:

www.dropbox.com

Supplier Contact details

To obtain the supplier contact details, log in to the Dropbox Business Continuity Account using your log in credentials:

www.dropbox.com

Client Contact Details

To obtain the Client Contact details log in to the Dropbox Business Continuity Account using your log in credentials:

www.dropbox.com

ITPS's Invocation details:

ITPS
Angel House
Drum Industrial Estate
Chester le Street
DH2 1AQ

Appendix 2

Signature of the Business Continuity Team and Company Directors who have read and approved the Business Continuity Plan

Name	Position	Signature	Date
Andrew Parker	Information Technology Leader		
Sean Hood	Applications Manager		
Neil McGlew	Financial Accountant		
Diane Charlton	Group Operational Manager		
Rob Charlton	Chief Executive		

APPENDIX D - Cyber Essentials Compliance Cert

CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

Space Group (Europe) Ltd

Spaceworks, Benton Park Road, Newcastle Upon Tyne, Tyne and Wear, NE7 7LX

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Chris Tait

CERTIFICATE NUMBER : IASME-CEP-004630

PROFILE VERSION : April 2020

SCOPE : Whole Organisation

DATE OF CERTIFICATION : 2021-07-15

RECERTIFICATION DUE : 2022-7-15

CERTIFICATION MARK

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.

{END OF DOCUMENT)