DATED

26TH APRIL 2017

VARIATION AGREEMENT

between

UNILEVER BUSINESS AND MANAGEMENT SUPPORT AG

and

THOROGOOD ASSOCIATES LIMITED

THIS AGREEMENT is dated

PARTIES

(1) **Unilever Business and Management Support AG**, a company existing in Switzerland, whose registered office is situated at Spitallstrasse 5, 8200 Schaffhausen, Switzerland (**"Unilever"**); and

(2) **Thorogood Associates Limited**, a company existing in England and Wales (registered number 021410616) whose registered office is situated at International House, 7 High Street, 2nd Floor NW, London W5 5DB (the **"Supplier"**).

BACKGROUND

(A) Unilever and the Supplier are party to a Framework Agreement for Consultancy and other Services dated 21st April 2011 (the **"Agreement"**), the Agreement was subsequently amended extending the Agreement until 31st May 2018.

(B) The parties wish to further amend the Agreement as set out in this variation agreement with effect from the date of this variation agreement (**"Variation Date"**).

In consideration of the mutual promises set out in this variation agreement, the parties agree as follows:

AGREED TERMS

1. VARIATION

1.1 With effect from the Variation Date the parties each agree the following amendments to the Agreement:

1.1.1 The following wording shall be added to the Agreement as a new Clause 27 (Information Security) immediately following Clause 26 of the Agreement:

> *"27 Information Security*
> *The Service Provider shall at all times comply with and adhere to the information security requirements set out at Schedule 10 of this Agreement (**Information Security Requirements**)."*

1.1.2 A new Schedule 10 (*Information Security Requirements*) shall be added to the Agreement as set forth in Attachment A hereto.

1.2 For the avoidance of doubt the above provisions shall take precedence in the event of any conflict with the above listed Agreement or any other contract existing between Unilever and the Supplier as at the date of this variation agreement.

2. GENERAL

2.1 This variation agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and interpreted in accordance with the law of England and Wales.

2.2 The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim that arises out of, or in connection with, this variation agreement or its subject matter or formation (including non-contractual disputes or claims).

2.3 No one other than a party to this variation agreement shall have any right to enforce any of its terms.

2.4 If there is an inconsistency between any of the provisions in the Agreement and this variation agreement, the provisions of this variation agreement shall prevail.

This variation agreement has been entered into on the date stated at the beginning of it.

Signed for and on behalf of
Unilever Business and Management Support AG

Name.....

Role.PROCUREMENT MANAGER

Signature...E.OXTOP.....

Date....3.5.17.....

Signed for and on behalf of
Thorogood Associates Limited

Name: JULIA HONIGSBERGER

Role..DIRECTOR.....

Signature.....

Date....26 APRIL 2017....

Attachment A

SCHEDULE 10

1. DEFINITIONS

In this Schedule 10, the following additional definitions apply, unless the context otherwise requires:

UGC	means any company that is an Affiliate of Unilever Plc or Unilever NV. "Affiliate" means in relation to a party any entity which, directly or indirectly, controls or is controlled by, or is under common control with, that party, where control is the possession, directly or indirectly, of (a) alone or pursuant to an agreement with other members, a majority of the voting rights in it, (b) the power to direct or cause the direction of the management or operating policies of the entity through the exercise of voting rights, contract, trust or otherwise, or (c) a right to appoint or remove the majority of the directors of the entity, and "Affiliates" means any of them
Unilever Data	means Data relating to any UGC or any supplier of any UGC provided or made available to Supplier or any other Supplier Group Company under this Agreement or any Local Services Agreement on or in any storage media (of whatever nature) whether in a human or machine readable form;, and shall include all Data generated pursuant to this Agreement by Supplier or any other Supplier Group Company to the extent it relates to a UGC or arises from the performance of the Services by Supplier or any other Supplier Group Company;
ISO 27001	means ISO 27001:2013, an information security standard that was published on 25 September 2013, published by the International Organization for Standardization and the International Electrotechnical Commission (as may be updated from time to time);
ISO 27001 Audit Results	shall have the meaning set out in Clause 2(b) of this Schedule 10;
Security Incident	occurs where (i) sensitive information including personal data is intentionally or unintentionally disclosed to an unauthorised environment or recipient, or (ii) there is an unauthorised access of Unilever Data Unilever Systems and /or devices, resulting in inappropriate use, falsification or an impact on availability;

Security Metrics Reports	shall have the meaning set out in Clause 4(a)(iii) of this Schedule 10;
Security Review	shall have the meaning set out in Clause 8(a) of this Schedule 10;
Statement of Applicability	means the statement defined under ISO 27001, which requires organisations to produce a Statement of Applicability that lists the controls that have been selected to treat identified risks, and provides a justification for the inclusion of those controls, regardless of whether they have been implemented or not, and the status of implementation for the selected controls, and to link to relevant documentation showing how each control is (or will be) implemented;
Supplier Information Security Representative	means an employee nominated by Supplier to be a single point of contact in respect of Supplier's obligations set out in this Schedule 10 for the Term;
Unilever Systems	means the equipment, Software and other electronic, computer and information communications technology devices and equipment owned, supplied, operated and/or developed by any member of the Unilever Group and/or any of its sub-contractors as varied, updated and renewed from time to time including all networks, servers, hosted applications and data centres and any equipment contained therein.

2. **STANDARDS COMPLIANCE**

(a) The Supplier shall, and shall procure that Supplier's sub-contractors and each Supplier personnel shall, ensure that their security management in connection with the Services, at a minimum, is aligned with the "Controls" and "Implementation guidance" as defined and set out in ISO 27001, including clearly defined security responsibilities, processes for risk management, access control, authorisation and administration, security design and configuration management, audit and assurance.

(b) The Unilever information security team and its delegates may review and confirm the ongoing existence and compliance and/or review, assess and confirm the adequacy of security management of Supplier and/or any sub-contractor of Licensor in relation to the provision of the Services.

3. **SECURITY ORGANISATION**

(a) Supplier shall have an information security function, which has responsibility for ensuring good practice in relation to information security across the Supplier Group and in relation to the provision of the Services, including the publication of information security policies.

(b) The head of Supplier's information security function shall be responsible for information security across the Supplier Group and shall ensure that Supplier's corporate information security Policies is at all times observed by Supplier in the course of providing the Services.

(c) Supplier must appoint a single point of contact for information security, who is independent of, is not a part of and does not report into the project/operations team.

4. **GOVERNANCE AND REPORTING**

(a) The Supplier Information Security Representative shall:

(i) arrange security governance reviews with Unilever at the agreed frequency, where required by Unilever

(ii) have security policies and standards and with embedded security processes across the Services provided to Unilever that are consistent with the principles set out in this Schedule 10. The Supplier Information Security Representative shall clearly communicate

points of contact and escalation paths to Unilever to ensure priority security concerns are addressed; and

(iii) provide security compliance and reports in accordance with Schedule 10 (*Service Levels/ Key Performance Indicators/ relevant Unilever security baseline controls*) across all relevant Services provided to Unilever (**"Security Metrics Reports"**). The Security Metrics Reports shall provide executive summary level view, details of areas of concern and supporting remediation and action plans for areas of low compliance or concern. The format of the Security Metric Reports will be defined and agreed with the Unilever Security Team, and the Supplier shall provide quarterly Security Metrics Reports for governance forums in accordance with Schedule 10 (*Reporting*) and quarterly Security Metrics Reports for operational reviews.

(b) Penetration Testing and Vulnerability Scanning:

During the Term of the Agreement:

(i) Unilever may perform penetration testing on the supplier's systems no more than once every 12 months. The scope of the testing will be discussed and agreed with the Supplier in writing, in advance. The Supplier will secure the necessary third party permissions required for Unilever to perform the penetration testing including, without limitation, its cloud services providers.

(ii) Supplier shall comply with the Unilever requirements on vulnerability scanning as contained in Unilever's Threat & Vulnerability Standard. Supplier shall permit all scans originating from Unilever's Scanner IP address and / or provide all its own vulnerability scan reports to Unilever.

(c) Supplier shall arrange for appropriate infrastructure and application security tests to be undertaken by a mutually agreed third party. The scope and frequency of the tests shall be agreed between the Supplier and Unilever in line with the risk profile of the systems in scope, and documented as a formal testing schedule. In addition, all public facing systems and services (e.g. websites, file servers) must be penetration tested before go live, and on an annual basis henceforth.

(i) Upon identification of vulnerabilities on the Supplier' maintained IT Systems, the Supplier will remediate such vulnerabilities in accordance with a mutually agreed remediation schedule. A decision not to remediate any vulnerabilities must be subject to approval from Unilever.

(ii) Supplier shall provide mutually agreed metrics at an agreed frequency to illustrate the performance of the testing schedule.

(d) Supplier shall continuously assess security risks to the Services and report any changes in such risk status immediately with detailed assessment and recommended mitigation controls and actions to the Unilever Security Team. Any urgent risks must be highlighted by the Supplier Information Security Representative to Unilever immediately on identification of such urgent risks.

5. **INCIDENT MANAGEMENT**

(a) Supplier shall inform Unilever of any known or suspected Security Incident, that affects, or has the potential to affect, the security of Unilever Data.

(b) Supplier shall ensure that all Security Incidents are dealt with in accordance with Unilever's incident management processes.

(c) Supplier shall:

(i) ensure Security Incidents are reported to a Unilever and Supplier single point of contact;

(ii) specify requirements for the recording of Security Incidents;

(iii) include categorising Security Incidents by type and prioritising them according to their impact / urgency; and

(d) Supplier shall provide confirmation to Unilever within thirty (30) days of execution of the Agreement that all its sub-contractors are bound to notify them of any known or suspected Security Incident. Supplier must notify Unilever immediately upon receipt of such notification from a sub-contractor.

(e) Supplier shall immediately report to Unilever all identified attempts (whether successful or not) of which it becomes aware by unauthorised persons (including unauthorised persons who are Supplier Personnel) either to gain access to or interfere with Unilever Data or Unilever Systems.

(f) Following any actual or suspected Security Incident, Supplier shall notify Unilever within 24 hours. The Supplier shall investigate and report to Unilever on the cause of the breach, including proposed corrective action within 36 hours of the incident. Unilever shall, where reasonably requested by Supplier (or, if not so requested, at its discretion), provide reasonable co-operation and assistance in connection therewith.

(g) In the event of an actual Security Incident, the Supplier must, in accordance with agreed Unilever Take Down Procedures, immediately upon request:

(i) not access or alter compromised system(s) in any way, including without limitation, not logging in to the compromised system(s), not changing passwords or not logging in to ROOT

(ii) isolate the affected system from all networks and preserve all evidence and logs; and

(iii) document all actions taken to contain, investigate and remediate the Security Incident, including dates, times and individuals involved.

(h) Supplier shall provide all reasonable co-operation, at its own cost, with any investigation relating to Security Incidents which is carried out by or on behalf of Unilever or any UGC and, if requested by Unilever or any UGC, Supplier shall, for the purposes of the investigation provide all documents, records or other material of any kind which may reasonably be required for the purposes of the investigation. Unilever and the relevant UGC shall have the right to retain copies of any such material to the extent required for the purposes of the investigation

6. **ACCESS MANAGEMENT**

(a) Where Supplier provides Services connected directly to Unilever Systems, Supplier shall be responsible for validating the identity of Supplier personnel. Supplier must keep Unilever appraised of the names of Supplier personnel and the required and actual levels of access to Unilever Data (including sub-contractors).

(b) Supplier shall ensure that individual named Supplier personnel at all times, have the minimal required system access to carry out their duties. Supplier shall not use shared privileged accounts.

(c) Supplier shall ensure that access to the Unilever Systems Data are governed by the security controls set out or derived from Supplier Security Policies and

Standards and that breach of the access control Policies leads to the threat of disciplinary action against Supplier Personnel.

(d) Supplier shall ensure that relevant Supplier Personnel are assigned a set of access privileges to allow them to read or change particular information or systems, only in accordance with their role requirements, any changes to these privileges shall be undertaken in accordance with the suppliers change control procedures.

7. **ASSET MANAGEMENT**

(a) **Asset Inventory.** Supplier maintains an inventory of all media on which Unilever Data is stored. Access to the inventories of such media is restricted to Supplier personnel necessary to provide the service(s).

(b) **Asset Handling.**

(i) Supplier classifies Unilever Data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

(ii) Supplier imposes restrictions on printing Unilever Data and has procedures for disposing of printed materials that contain Unilever Data.

(iii) Supplier personnel must obtain Supplier authorization prior to storing Unilever Data on portable devices, remotely accessing Unilever Data, or processing Unilever Data outside Supplier's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Unilever Data from Supplier's facilities.

8. **POLICY AND PROCESS**

(a) Supplier shall have documented information security policies and standards, approved at a sufficiently senior level within Supplier organisation to ensure corporate compliance. The information security policy shall apply to all Supplier Personnel and their use of data, information and systems. Supplier shall appoint an individual (or a group of individuals) within the Supplier Group who shall be responsible for maintaining the information security policies and standards.

9. **SECURITY REVIEW**

(a) Supplier shall permit Unilever personnel, authorised representatives and any party to whom Unilever is legally obliged to provide access or audit rights ("**Reviewers**"), to review and assess Supplier's compliance with the obligations set out in this Schedule 10 ("**Security Review**").

(b) The Reviewers shall be entitled to, in respect of Supplier, and / or its sub-contractors, access the premises controlled by them, extract any Unilever Data held on their Systems, inspect their security risk management controls

and procedures, and interview Supplier Personnel in order to assess compliance with the obligations set out in this Schedule 10.

(c) Subject to paragraph (d) below, Unilever shall be entitled to conduct a Security Review in accordance with this Clause 9 no more than once per annum.

(d) Where Unilever has reasonable grounds to suspect breaches of the security of Unilever Data or Unilever Systems by Supplier, its sub-contractors, or third parties which have obtained unauthorised access to Unilever Systems via Supplier's Systems, Unilever may exercise the rights under this Schedule 10 in relation to the Supplier Systems connected to the potential breach upon service of no less than 24 hours advance, written notice.

(e) Supplier and/or its sub-contractors (as applicable) shall remediate any failures identified by the Security Review as directed by Unilever, including developing a comprehensive remediation solution for identified gaps and obtain Unilever approval for implementation. The cost of remediation shall be borne by the Supplier and/or its sub-contractors (as applicable).

(f) Supplier shall remediate any failures identified by the Security Review as directed by Unilever.

10. SUB-CONTRACTORS

(a) Subject to any provisions in the Agreement, Supplier shall not sub-contract, assign, or otherwise delegate any of its responsibilities of this Schedule 10 unless agreed with Unilever in writing, in advance. For the purposes of this Schedule, any third party that Unilever contracts with directly in relation to the Programme shall not be considered a sub-contractor of the Supplier, and the terms of this Section 10 shall not apply in respect of such third parties.

(b) Where Supplier is permitted by Unilever to sub-contract any of its obligations under this Schedule 10, Supplier shall remain Unilever's sole point of contact for all matters falling within the scope of this Schedule 10, and shall procure that its sub-contractor complies with and is bound by the requirements of this Schedule 10 as they apply to Supplier. Supplier shall be responsible for all acts and omissions of each of its sub-contractors which shall be treated as if they were the acts or omissions of Supplier itself.

(c) Supplier shall procure that all sub-contractors used by it in the provision of the Services from time to time under this Agreement execute a confidentiality undertaking on terms that are substantially the same as (and no less onerous than) those set out in the Agreement.

(d) Unilever may revoke its prior approval of a sub-contractor (including an Approved Sub-Contractor) where, in Unilever's reasonable opinion, the performance of the sub-contractor is materially deficient or in the event of any material breach by the sub-contractor of the terms of this Schedule

11. BUSINESS CONTINUITY MANAGEMENT

(a) Supplier shall have a documented Business Continuity and Disaster Recovery Plan (BC DR Plan) throughout the Term, a copy of which is attached as appendix 1 to this Schedule 10 in place which shall be tested at least annually and the results of the test along with gaps, corrective action plan and timelines for action shall be shared with Unilever.

(b) Supplier maintains emergency and contingency plans for the facilities in which Supplier information systems that process Unilever Data are located.

(c) Supplier's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Unilever Data in its original state from before the time it was lost or destroyed.

12. OBLIGATIONS ON TERMINATION

(a) Upon termination or expiry of the Agreement, Supplier shall, as requested by Unilever, either:

(i) promptly and securely destroy any Unilever Confidential Information and other Unilever Data in its possession. However, Supplier shall retain and properly store during the term of the agreement and following termination or expiry for at least 7 years all financial information required by Law; or

(ii) promptly purge its systems of, and deliver to Unilever, in Unilever's chosen format, on media free of viruses, within five (5) days of the date of termination of the Agreement and / or applicable Order Form, all copies of the relevant Unilever Confidential Information in the possession or control of the Supplier.

and shall provide written confirmation of the action taken under (a) and/or (b) above within 7 days.

(b) No Unilever Asset or Data shall be retained by the Supplier unless approved by Unilever in writing, in advance.

(c) All the desktops and servers shall be formatted and cleaned by the Supplier before they are put to reuse.

Thorogood Associates

Business Continuity Management Plan

Distribution list:

Thorogood Associates Inc	US Management Team for cascade
Thorogood Associates Ltd	UK Management Team for cascade
Thorogood Associates Pvt Ltd	India Management Team for cascade

Version control:

Number	Comments
01	Original version FY 2009
02	Previous Version FY 2012
03	Previous Version Jul 2015
04	Current Version Nov 2016

If you have any suggestions for changing this plan, please contact:

Caroline Gore
t : 0208 231 0807
e : caroline.gore@thorogood.com

Contents

1. Introduction

This plan is designed to prepare Thorogood to cope with the effects of an emergency or crisis, so that business operations can continue.

2. Objectives of the plan

- To explain the critical activities
- To review the risks that need to be managed
- To lay out an action plan in detail
- To identify key roles, responsibilities and contacts

3. Critical Activities Checklist

As a professional services firm Thorogood has a relatively low dependence on fixed facilities, transport or logistics of the kind which are most vulnerable to accident, acts of god, terrorist action or pandemics. Our people can operate effectively from remote locations, including their homes, using modern telecommunications and internet links. All staff members have home broadband, mobile phones, and laptop computers. These communication links are already extensively used for web conferencing and joint working between our globally distributed personnel and make our communications resilient and robust under most disaster scenarios.

Our policy is to use external service providers for infrastructure services as far as possible because such providers enjoy economies of scope and scale and offer resilience. Accordingly we have an external e-mail service with 'MimeCast' and external telephone conference service with "Intercall". We use multiple parallel telephony services; PSTN, mobile and VoIP - everyone has mobiles and landlines.

However, for efficiency we also have our own fixed infrastructure facilities such as network and intranet servers so these are also structured for resilience. We have duplicated our resources over two data centres, one in Bangalore India and one in London in the UK with fail-over arrangements between the two. The sites operate mutual back-up, mirroring and fail over procedures so that full facilities can be restored promptly should one of the sites fail or become inaccessible.

As well as working with our clients' development environments (to which we mostly have remote access) we also have our own duplicate development environments. This means that we can continue development work even if a client has a problem which makes access to client sites or systems infeasible.

The focus of our business continuity plan is to coordinate appropriate recovery activities across the firm to any incident which threatens normal working.

Each of the activities that are critical is examined in more detail below. This provides a checklist to ensure that critical tasks are completed on time and according to a pre-agreed priority schedule. This list is to be used as a hand-over document between different responsibilities in the recovery process.

4. Command and Control

The decision to use this plan will be taken by the Thorogood Executive Team, and they will also be responsible for making any key decisions required in the course of the response.

5. Critical Activities and the Recovery Process

Priority:	1	Critical Activity:	Voice/Text/E-mail Communications
Responsibility:			Peter Thomson - Infrastructure Manager
Potential impact on organisation if interrupted:			High
Likelihood of interruption to organisation:			Very Low: e-mail will fail over to a third party supplier (MimeCast). All staff members have home broadband and mobile telephones and the services of an external conferencing provider.
Recovery timeframe: *(how quickly must this capability be recovered to avoid lasting damage)*			Redirecting client calls and communications to an alternative site is immediate.
Resources required for recovery:			
Staff *(numbers, skills, knowledge, alternative sources)*			Infrastructure team members in either India or the UK can take action to redirect client calls via the alternative site, and post implementation can check that communications are operating normally.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*			E-mail service via MimeCast and multiple telephony options in place.
Premises *(potential relocation or work-from-home options)*			Alternative sites are Ealing, Philadelphia, Jersey City, and Bangalore. Each country has work from home options.
Communications *(methods of contacting staff, suppliers, customers, etc)*			Telephone, e-mail, mobile voice and data Also see Section 7 Contact Lists.
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*			Key equipment is in place. All staff have laptops All staff have home broadband All staff have mobile phones
Supplies			Internet calls and internet e-mail communications can be maintained if mobile and 3G networks become overloaded.

Priority	2	Critical Activity	Establishing Staff Status, act as information point for staff and family members

Responsibility: *(role responsible for leading on this activity, plus deputies)*	Emergency Response Team (see Emergency Response Plan)
Potential impact on organisation if interrupted:	Potential impact on staff morale and company reputation if uncertainty persists about status of staff
Likelihood of interruption to organisation:	High
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*	2 hours
Resources required for recovery:	
Staff *(numbers, skills, knowledge, alternative sources)*	Emergency Response Team (see Emergency Response Plan)
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*	All staff and next of kin to be contacted to establish status using contact lists with next-of-kin details. (Assume intranet is not available.) Liaise with emergency services and local authorities.(Details in Emergency Response Plan)
Premises *(potential relocation or work-from-home options)*	Not dependent on premises
Communications *(methods of contacting staff)*	e-mail, mobile telephony and VoIP Also see Section 7 Contact Lists.
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*	Key equipment in place. All staff have laptops All staff have home broadband
Supplies *(processes to replace stock and key supplies required; provision in emergency pack)*	Use internet calling if mobile networks become overloaded

Priority 3 Critical Activity	**Restoring Shared Files**
Responsibility: *(role responsible for leading on this activity, plus deputies)*	Peter Thomson and Binesh Maroli in charge of daily back-ups and daily replications (for key shared files and virtual machines). I think we would mention Druve here, as this is not talking about VMs?
Potential impact on organisation if interrupted:	High. We will lose up to 24 hours of work that has not yet been replicated or backed up since the last daily replication or back-up.
Likelihood of interruption to organisation:	Low
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*	Replication for important files and VMs is immediate but can take 48 hours to restore data files from daily backup
Resources required for recovery:	
Staff *(numbers, skills, knowledge, alternative sources)*	Peter Thomson in UK, Binesh Maroli in India.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*	Daily back-up tapes stored in safety deposit vaults (Iron Mountain)
Premises *(potential relocation or work-from-home options)*	Fail over from using servers at affected site to servers at alternative site
Communications *(methods of contacting staff, suppliers, customers, etc)*	E -mail telephone and data communications
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*	Fail over servers located in UK (1 site) India (1 site)
Supplies *(processes to replace stock and key supplies required; provision in emergency pack)*	Back-up tapes and emergency pack stored offsite in a safety deposit vault (Iron Mountain)

Priority	4	Critical Activity	Alternative Representative Offices
Responsibility: *(role responsible for leading on this activity, plus deputies)*			General Managers, Office Managers
Potential impact on organisation if interrupted:			Low. We will incur additional travel time and expense to alternative locations.
Likelihood of interruption to organisation:			Low
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*			Immediate physical relocation possible, immediate for telephony, 48 hours to restore shared data files.
Resources required for recovery:			
Staff *(numbers, skills, knowledge, alternative sources)*			Office managers to open up alternative locations.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*			Air con, utilities, office services all in place in alternative sites
Premises *(potential relocation or work-from-home options)*			Staff will have the option to attend alternative offices or work from home.
Communications *(methods of contacting staff, suppliers, customers, etc)*			E -mail and telephone
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*			Servers, phones communications links are provided at all alternative sites
Supplies *(processes to replace stock and key supplies required; provision in emergency pack)*			Stationery, office supplies and office facilities are available at all alternative sites.

Priority	5	Critical Activity	Virtual Machines
Responsibility: *(role responsible for leading on this activity, plus deputies)*			Project Managers, Peter Thomson, Binesh Manoli maintain copies of all virtual machines on servers at mirror site.
Potential impact on organisation if interrupted:			High. We would lose any work done on the virtual machines between daily replications.
Likelihood of interruption to organisation:			Low
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*			24 hours to recreate all virtual machines from mirrored machines.
Resources required for recovery:			
Staff *(numbers, skills, knowledge, alternative sources)*			Peter Thomson in UK, Binesh Manoli in India.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*			Daily back-up of virtual machines
Premises *(potential relocation or work-from-home options)*			Fail over from affected sites to alternative sites
Communications *(methods of contacting staff, suppliers, customers, etc)*			E -mail and telephone
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*			Virtual machines available for mirroring in in UK (1 sites) and India (1 site)
Supplies *(processes to replace stock and key supplies required; provision in emergency pack)*			SAN holds mirrored virtual machines

Priority	6	Critical Activity	Access to Development Environments
Responsibility: *(role responsible for leading on this activity, plus deputies)*			Project Managers, Peter Thomson, Binesh Manoli, a duplicate development environment is maintained (daily updates) for all current applications under development.
Potential impact on organisation if interrupted:			High. If we were unable to access the development environment we could lose development time.
Likelihood of interruption to organisation:			Low, since duplicate environments in place, but a potential loss of up to 24 hours of development work
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*			24 hours to recreate development status
Resources required for recovery:			
Staff *(numbers, skills, knowledge, alternative sources)*			Peter Thomson in UK, Binesh Manooli in India.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*			Daily refresh of duplicate development environments
Premises *(potential relocation or work-from-home options)*			Fail over from any affected sites to alternative sites
Communications *(methods of contacting staff, suppliers, customers, etc)*			E -mail and telephone
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*			Servers and storage available for duplicate environments in UK (1 sites) and India (1 site)
Supplies *(processes to replace stock and key supplies required; provision in emergency pack)*			Server capacity available

Priority	7	Critical Activity	**Remote Access to Client Sites**
Responsibility: *(role responsible for leading on this activity, plus deputies)*			Project Managers and Account Managers to ensure that remote access arrangements are agreed with all clients on all current projects and duplicate development environments are available.
Potential impact on organisation if interrupted:			High. We would otherwise lose the ability to progress current projects.
Likelihood of interruption to organisation:			Low
Recovery timeframe: *(how quickly must this function be recovered to avoid lasting damage)*			Alternatives to site access are routinely in place so lack of physical client site access should not be cause of more than one day delay to development programmes.
Resources required for recovery:			
Staff *(numbers, skills, knowledge, alternative sources)*			Project managers, account managers, infrastructure managers to set up remote access arrangements with clients.
Data / systems *(backup and recovery processes, alternative manual work-round, staff and equipment required)*			Security systems and procedures agreed to permit remote access.
Premises *(potential relocation or work-from-home options)*			Work from home if no access to client or office locations is available.
Communications *(methods of contacting staff, suppliers, customers, etc)*			E -mail,internet mail, PSTN, Mobile, VoIP conferencing communications
Equipment *(key equipment recovery or replacement processes; alternative sources; mutual aid)*			Remote access over VPN to client systems

6. Emergency Response Checklist

This page should be used as a checklist during the emergency.

Task	Completed (date, time, by)
Actions within 24 hours:	
Start of log of actions and expenses undertaken (see section 9 Action and Expenses Log)	
Confirm communication links are functioning as planned	
Establish status of all staff members	
Liaise with emergency services (see section 7E Contact List - Emergency Services)	
Identify and quantify any damage to the organisation, including staff, premises, equipment, data, records, etc	
Identify which critical capabilities have been disrupted (use section 3 Critical Activity Checklist)	
Convene those responsible for recovering identified critical capabilities, and decide upon the actions to be taken, and in what timeframes (use sections 4 Command and Control and 5 Critical Activity Recovery Process)	
Provide information to: • Staff • Suppliers and customers • Insurance company	
Daily actions during the recovery process:	
Convene those responsible for recovery to understand progress made, obstacles encountered, and decide continuing recovery process	
Provide updated information to: • Staff • Suppliers and customers • Insurance company	
Provide public information to maintain the reputation of the organisation and keep relevant authorities informed	
Following the recovery process:	

Arrange a debrief of all staff and identify any additional staff welfare needs (e.g. counselling) or rewards	
Use information gained from the debrief to review and update this business continuity management plan	

7. Contact Lists

The following sections shows the format of the contact details that are essential for continuing the operation of the organisation. This information is confidential and is included in the **emergency pack** that is secured offsite in Iron Mountain.

A. Staff

Name	Work phone	Home phone	Mobile	E-mail
Next of kin				
Next of kin				
Next of kin				

B. Key Suppliers

Supplier	Provides	Telephone	E-mail

C. Key Customers

Customer	Service / goods used	Telephone	E-mail

7. Contact Lists (continued)

D. Utility Companies

Utility	Company	Telephone	E-mail
Electricity			
Gas			
Telecommunications			
Water			

Include a plan of your premises (for use by emergency services) showing locations of:
- Main water stop-cock
- Switches for gas and electricity supply
- Any hazardous substances
- Items that would have priority if salvage became a possibility

E. Local Emergency Services (UK)

	Location	Telephone
Ambulance	Emergencies	999
Fire Service	**Service**	999
Floodline	Information service	0845 988 1188
NHS Hospital	Ealing Hospital	
Medical Practitioners		
Police	Emergencies Local Stations	999

F. Insurance and Finance Companies

Service	Company	Telephone	E-mail
Banking			
Invoice Finance			
Insurance			

G. Local Authorities

London Borough of Ealing
24 hour helpline: (020) 8825 7468/6666
Website: www.ealing.gov.uk

8. Emergency Pack

An emergency pack of key items is held off-site in a safety deposit vault at Iron Mountain (who also holds daily server back-up tapes). This pack will be retrieved in an emergency to help in the recovery process.

GM's, office managers and infrastructure managers have access to the Iron Mountain emergency pack. The contents of the emergency pack comprise the following:

Contents:

- A copy of this plan.
- Key contact details listing.
- Copy of the Insurance policies.
- Daily Back-Up tapes and disks.
- Duplicate keys to sites and alternative sites.
- Plans of the premises for the emergency services
- Duplicate Financial records
- Spare 3G network cards

9. Actions and Expenses Log

A log of events, decisions and outcomes should be kept to provide information for the post-recovery debriefing and to provide evidence of costs incurred for any claim under an insurance policy. A form (below) can be used to record decisions, actions and expenses incurred in the recovery process.

Date/time	Decision / action taken	By whom	Costs incurred

I have read and understood this policy