

Business Continuity and Disaster Recovery Plan

Date: September 2026

Co-ordinated by: Andrew Norris, Managing Director

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	1 of 9

Contents

1. Purpose of plan
2. Responsibility/accountability
3. Risk Treatment
4. Scope of Plan
5. Procedures
 - 5.1 IT and Communications Failure
 - 5.2 Building Access Restrictions and Building Loss
 - 5.3 Loss or illness of key staff;
 - 5.3.1 Outbreak of disease or infection
 - 5.4 Fuel Shortage
 - 5.5 Power Cut
 - 5.6 Theft and/or vandalism to property and fire
6. Implementation
7. Consultation/communication
8. Validation

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	2 of 9

1. Purpose of Plan

It is vital that we can commit to meeting our customer's demands, irrespective of any external factors which may impact on our business. Our policy has been formulated with careful consideration, to give a structure and process which will enable staff to continue with day to day operations with minimal impact to our clients. The policy will be reviewed annually and is tested annually to ensure that the plans outlined are feasible, realistic and deliver the continuity which is our aim.

This document outlines the actions and procedures to ensure continuation of operations providing as complete a service as possible to all our Clients and how the system should be managed, for dealing with potential crisis events, along with named staff for dealing with potential crisis events.

2. Responsibility/accountability

The Business Continuity and Disaster Recovery policy has a nominated accountable Director, Mr Angus MacInnes, and a nominated continuator co-ordinator, Mr Ian Nairn. Both members of staff review this document considering any operational changes and communicate changes. They are tasked with reporting any relevant issues to the Board of Directors.

3. Risk Treatment

When analysing the risk, we consider the probability and consequence of the events which could affect our business and our clients in a negative way. We use a numerical scale to quantify the potential impact of crisis and decide on the course of action; a technique which follows industry best-practice.

Probability and possible consequences for each factor are scored. Probability ranges from very unlikely to highly likely, consequence ranges from minimal to severe. The scores are multiplied to give an impact score which is then analysed.

Impact scores of between 1 - 5 are considered to be small. The event is unlikely to occur, and if it did, the consequence would be so minimal that mitigating actions are usually negligible.

Impact scores between 6 - 20 are likely to have a significant impact so mitigating actions are considered, planned and reviewed. The level of detail and resource invested increases with the score.

Impact scores of 21+ are considered an unacceptable risk to business continuity and immediate action is required to reduce the score. Once the action has been taken and the score has reduced, the process for scores 6 - 20 is followed.

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	3 of 9

Business Continuity & Disaster Recovery Plan

4. Scope

The policy covers the following areas:

- IT and communications Services Failure
- Utility Failure
- Building Access Restrictions and Building Loss
- Loss or Illness of Key Staff, Outbreak of Disease or Infection
- Fire to Premises
- Fuel Shortage
- Theft and/or Vandalism of Company Property

5. Procedures

5.1 IT and Communications Services Failure

Our IT Consultant TMS Ltd, provide us with both pro-active and re-active protection of our IT systems and processed under a standard maintenance agreement and a 4-hour server crisis recovery.

Taylor and Fraser's "Real Time" Document Management System is core to the Company's entire business operation to ensure business continuity throughout. The Document Management System catalogues all categories of each project/contract that Taylor and Fraser undertake, from the contract number, correspondence, drawings, tender documents, and so forth. In the event of a major incident where Taylor and Fraser's premises become un-operational due to a major incident, the Company has a disaster recovery process in place that would ensure that the Company is up-and-running through Taylor and Fraser's remote IT capability.

Procedures:

- Quantum will provide a 4 hour disaster recover service and will have the server in full operation within 4 hours so that day to operations can continue
- The system is backed up in 'real-time' throughout the day, every working day, with a 'full' back-up in the evening.
- A backed-up cassette is taken off-site every day and kept in a safe place by a member of the Management Team.

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	4 of 9

Business Continuity & Disaster Recovery Plan

- A backup Server which is in a separate building operates a complete duplicate of the system which is now on the main server. In the event of a fire, theft or operational failure this remote server can be made operational immediately.
- All Management staff and key operational staff have their own laptop, which has access to the Company's server, which can be used remotely which also allows for business continuity.
- All electronic documentation received and generated by the Company is automatically saved through the Document Management System, ensuring that no documentation is lost in the event of a major incident.

These procedures have been audited by various accreditation bodies for ISO9001, ISO14001, ISO45001, CHAS, SSIP, BM Trada and Zurich Insurance all of which have praised the Company on its unique and comprehensive approach to Disaster recover.

5.2 Building Access Restrictions and Building Loss

There is the possibility, that access to the building may be restricted due to adverse weather conditions such as snow and ice. It may also be the case that the use of our headquarters is not possible due to utility failure or fire.

Procedures: • In the event that the premises from which we would normally undertake our business operations are unavailable, we have the capacity to operate from any one of our sites or where applicable from home.

- Storage facilities are available, including offices with remote access to the company's servers and data (through Quantum) and capacity for the use of key staff.
- Key staff (refer to point 5.3 for further details) will then take charge of company dealings. We expect that any event such as this, would compromise our dealings with clients for no more than a 48-hour period, with normal functioning of our operations following immediately after.
- The company has multiple storage of contact details for its clients and staff, so communication throughout will remain constant.
- The company's insurances mean that in the medium term, alternative premises can be provided to allow us to return to normal working conditions.

5.3 Loss or illness of key staff:

In the event that one of our key staff becomes long term ill, ceases to work for the company, is involved in a fatal accident or passes away from natural causes, the company will be able to continue

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	5 of 9

Business Continuity & Disaster Recovery Plan

and fulfil its contractual obligations. A list of key staff with their contact details is shown hereunder, along with arrangements for cover:

Name	Role	Replacement
Andrew Norris	Managing Director	T&F Board
William McGill	Engineering Director	Ian Nairn
Angus MacInnes	Construction Director	Ruairidh MacLennan
Emma Devnani	Head of Finance	Joanne Whiteford

Each replacement member of staff shown has previously been employed in the role they are expected to cover and are absolutely capable of undertaking the tasks required of them when undertaking this job role.

In the event that more than one of our key staff is no longer with the company, permanent replacement will be arranged through our agencies, and extensive contacts within the industry.

Name	Role	Contact number
Andrew Norris	Managing Director	+353 (057) 756 7726
William McGill	Engineering Director	07702 636495
Angus MacInnes	Construction Director	07909 528717
Enma Devnani	Head of Finance	07345 467682
Ian Nairn	Commercial Director	07717 507102
Ruairidh MacLennan	Senior Quantity Surveyor	07825 409757

Nominated Accountable Director – Angus MacInnes

Nominated Continuity Coordinator – Ian Nairn

5.3.1 Outbreak of disease or infection:

The following groups are more vulnerable to the consequence of disease outbreak and will be protected as much as is reasonably practicable if an outbreak of any disease occur by use of isolation or home working.

These conditions include:

- Asthma
- Cardiovascular disease

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	6 of 9

Business Continuity & Disaster Recovery Plan

- Diabetes
- Autoimmune disorders and obesity
- Pregnant women may have an increased risk of complications especially in the second and third trimester
- New mothers
- Older and frail people

Procedures:

Where offices have confirmed cases of any notifiable infection all people identified as within a vulnerable group will be isolated from infected parties.

Each manager is responsible for identifying employees who have conditions that categorise them as vulnerable people and then identifying suitable working conditions for each individual.

5.4 Fuel Shortage

Disruption to our fuel supply could occur for a number of reasons: Scarcity of supply, technical problems with the fuel infrastructure, Industrial action / public protest. In the event of any of the above, the situation could be worsened by panic buying. A worst-case scenario is that petrol stations and commercial supplies could be exhausted within 48 hours of an incident, and it could take up to 10 days before stock levels are fully restored.

Procedures:

If a fuel shortage occurs, we shall be able to fulfil our contractual obligations, through adherence to the undernoted measures. Our own Head Office has a fuelling tank (of 40,000 litres) and we would reduce our dependency on it by:

- Encouraging car sharing
- Cancellation of non-essential journeys to enable us to fulfil our essential services improving the resilience of company supply chains.
- Re-allocation resources to deliver only key products and services
- Effective communication with staff, customers, suppliers and other key stake holders in advance of, and during a major fuel disruption.

5.5 Power Cut

In the event of a power cut, we have an uninterruptible Power Supply connected directly to the server which provides for monitoring and management via the APC Powerchute application. Quantum

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	7 of 9

monitor the status of the UPS and logged events, such as fluctuations in power supply, outages and battery condition, on an ongoing basis under the maintenance agreement.

5.6 Theft and/or vandalism of company property/Fire

In the event that any of the above should occur, we have appropriate measures in place to protect our employees, property and assets and ensure the continuity of our day-to-day business operations. The Company has an intruder alarm to monitor and detect unauthorised entry and also has a surveillance system with external CCTV surveillance cameras and a fire alarm installed in the building in the event of fire occurring. The intruder alarm system is connected to the local police force and the fire alarm to the local fire services. The police and/or fire services will visit the premises in the event that the alarm(s) are activated, follow appropriate procedures and take any necessary action(s). The external CCTV cameras are connected to a monitoring centre.

6. Implementation

The activities to ensure business continuity and disaster recovery will be implemented according to the policy. Although the policy has never been required in a "live" situation it is robustly tested so staff are familiar with the procedures.

Taylor and Fraser undertake period testing of the plan with particular focus on the possibility of IT and communications failure. Short- and medium-term actions include escalation to senior staff (including out of hours notification by telephone and contact with external contacts (such as customers, and business partners).

The final stage of implementation is a review and lessons learned phase which may result in updating this policy.

7. Consultation and Communication

We consult with our employees on business continuity and disaster Recovery Information instructions and advice on an on-going basis. The policy is communicated to staff during their workplace induction and is in the Employee Company Handbook. This covers the contents of the policy, the individual's own responsibility with respect to the policy, and the methods by which they will receive updates. Thereafter the policy is kept up to date on the intranet and by the following means:

- Company briefing notes/newsletters
- Noticeboards
- Toolbox talks
- Company Meetings
- Internal Memorandums

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	8 of 9

- E-mail mail shots
- Posters and leaflets

8. Validation

The events that have been identified, and the resultant policy, have been approved by independent auditors from SGS (for ISO9001, 14001 and 45001) and Zurich Insurance.

On a day-to-day level, the policy is tested using several methods. By way of example, Mr MacInnes will challenge the directors to recount the procedure to follow if they receive a disaster phone call. Mr Nairn will ensure the remote IT connections are tested on a weekly basis. The operations team will carry out scenario planning for dealing with loss of building access.

Name: Andrew Norris Position: Managing Director

Signed:  Date: 03.09.2026

Revision	Description	Reviewed by	Approved By	Date	Page
No: 01	Updated Document	CS	SMT	20.08.2026	9 of 9