Bridge Digital Agency

31 All Saints Close, March
Cambridgeshire, PE15 8US
07738482216
info@bridgedigitalagency.net

April 2020

We want to ensure that all of our clients have peace of mind about their projects with us and know that we take every precaution to make sure your data is safe and secure. Below you will find details about how you will gain access to your data and assets in the event of our business failing, natural disaster or permanent loss of staff.

Best regards,

Scott Mokler

Director, Bridge Digital Agency Ltd

Natural Hazards

Extreme weather conditions

In the event of extreme weather all employees will be asked, where possible, to work from home. All meetings will be held online via services such as Zoom where possible. Clients will be notified that this action has been taken and contact details for our staff while working remotely will be made available.

In the event of weather conditions causing power outages or internet access issues we will do our best to provide mobile internet access for those staff affected.

Technological failure

Infrastructure failure

Nearly all of our services are located off site. Where possible all of our services are cloud based which are scaled across multiple physical servers. In the event of one physical server having hardware issues there should be little to no downtime.

All of our hosting comes with daily backups included in the charge. These backups are complete server images so that if need be we can clone the server via the image within minutes. We have hourly scripts in place that will take a backup of all of our clients databases and will store them both locally on the server and on a separate file server. This is to ensure that there is not a complete data loss in the event of hardware failure.

All of our current development projects are worked on locally rather than on remote servers. This is for speed and consistency reasons as our local development environments allow us to be flexible. We ensure that our development environment matches as closely as possible with your remote server software versions. Where this is not entirely possible we run software called Vagrant which allows us to create a local development server with the exact software of your remote server.

All of our code is stored remotely via version control software either on GitHub or BitBucket. These are secure and reliable platforms serving millions of users ranging from small to multimillion pound projects like Facebook.

Our local machines are all Apple Mac and we use their backup software called Time Machine. This provides hourly, daily and weekly backups of all data stored on our machines. Should anything happen to our local machines then we will provide new machines as soon as physically possible and using Time Machine they can be restored to the latest backup version swiftly.

Human Caused/Based Events

Cyber Security

We take security very seriously. All of our servers are only accessible via certain ports, everything is locked down other than that. Port 80 and port 443 are left open for web connections for example. We only enable port 22 for clients that specifically require FTP access but advise against it. We do not enable software on our servers that are known to have security holes, for example the database management system phpMyAdmin. In situations where software like this is required and there is no viable work around, access to this software will only be permitted via the required users IP address via the server firewalls to limit the risk of intrusion.

We regularly run security checks and updates where required on the servers. When this will have an impact on downtime we will advise customers. These checks are performed on both server software and web application software. This is included in your support contract if you have one. If you do not have a support contract with us then any maintenance work that is required will be charged at our hourly rate.

All of our local machines are setup so that the hard drive is encrypted. In the event of our laptops being lost or stolen it is very unlikely that anyone would be able to gain access to any of the data stored on our machines. The same goes for our backup drives.

All of our account access for providers have been setup with two-factor authentication software where possible. In the event of staff leaving the company access to all services is immediately terminated and where needed passwords changed.

All of our passwords are stored in the secure password management system 1password. Access to this is limited to users via email address and only passwords that the user will need to be able to perform their job role will be provided to them. All passwords are generated randomly and include a minimum of 8 characters including special characters and numbers to increase security.

In the unlikely event of a data breach, all passwords for all services will be immediately changed. The cause of the breach will be investigated and where required patches to security will be applied. If the breach is based on human error where it is genuinely a mistake, training will be given to the staff member to prevent repeat issues. Full code reviews will be applied to all code that has been developed up to 6 months prior to the event.

Where the event is caused intentionally by gross negligence or misconduct the staff member will immediately be terminated from employment and legal action will be taken where required as set in the terms of employment.

Complete loss of staff.

In the very unlikely event of a complete loss of staff we have appointed an external developer to help transfer control of all customer data to all of our customers. This developer will create an export of all database content, cron jobs, server settings and website code. Usernames and passwords for anything other than these items listed will not be provided to protect security (for example, a user for a staff member at Bridge Digital Agency Ltd that is not required for you to administer and maintain your project will not be provided. It will be recommended that you remove these users as soon as you have complete control over your project). In the event of a complete loss of staff you will be informed as soon as possible by this developer and he will trigger the transfer process once you have set up a new provider.

Company ownership

Currently the company is owned solely by Scott Mokler. While this may change in the future the current plan of action in the event of a fatality or serious illness is that the company ownership gets transferred to Kirstie Mokler. If the company is unable to proceed trading either by knowledge limitations or technological limitations then Kirstie Mokler will be able to provide all clients with access to their services, code etc and then dissolve Bridge Digital Agency.

If Bridge Digital Agency is able to continue trading and providing services to our clients then Kirstie will either take the role of Managing Director or appoint someone to this role.

Document Version History

Date	Version	Editors Initials	Checked by
21/04/2020	1	KM	SM
11/06/2020	2	KM	SM