Disaster Recovery Plan

Bottega University
50 W Broadway, Suite 300
Salt Lake City, Utah 84101

1. Major Goals of this Plan

- To minimize interruptions to normal business operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth restoration of the headquarters facility.

2. Personnel

Technology/Senior Personnel			
Name	**Position**	**Location**	**Contact Information**
Dr. Mary Beth Finn	President (Senior Personnel)	Lake View, AL	(c) 205.482.3071 mfinn@bottega.edu
Dr. Troy Roland	Academic Dean/Compliance Officer (Senior Personnel)	San Diego, CA	(c) 619.549.8096 troland@bottega.edu
Kelly Shearer	Admissions Director (Senior Personnel)	Spotsylvania, VA	(c) 540.847.9216 kshearer@bottega.edu

In addition to the personnel noted above, there are additional remote/offsite personnel capable of assuming roles in the Disaster Recovery Procedures. Bottega's President will be responsible for assigning such roles. All personnel have been trained and use the decentralized systems noted in section 3.

3. Hardware/Software Assets

Onsite/Headquarters		
Hardware/Software Name	**Critical? Yes/No**	**Comments**
Router	Yes	Owned/managed by property manager
Computer	Yes	
VoIP Phone	Yes	Owned/managed by property manager
Printer	No	
Filing Cabinet	Yes	Fireproof Cabinet with combination locking feature

Offsite			
Hardware/Software Name	**Critical? Yes/No**	**Contact Information**	**Comments**
OVH Server	Yes	OVH.com	Offsite Server for BU Website and Cloud Storage
Box.net	Yes	Box.net	Offsite Cloud Storage for Student Files
Jack	Yes	Jack.new.edu	Offsite Cloud Storage for Student Files
Google Suites	Yes	Google.com	Google managed office suite products and cloud storage.
Bottega University Website	Yes	Bottega.edu	Digital Ocean
Quickbooks Online	Yes	Qbo.intuit.com	Online Accounting Software
AspireEDU	Yes	Aspire.com	Online instructor and

			student analytics program
Diamond SIS	**Yes**	**Diamond.com**	**Student Information System, managed by vendor**
Canvas LMS	**Yes**	**Bottegauniversity.Instructure.com**	**Learning management software, managed by vendor**
ProctorFree	**Yes**	**ProctorFree.com**	**Proctoring service managed by vendor**
Turnitin	**Yes**	**Turnitin.com**	**Plagiarism software detection managed by vendor**
ProQuest Library	**Yes**	**Proquest.com**	**Research library embedded into LMS, managed by vendor**
Personal Computers	**Yes**		**Personal Computers for Staff**
Telephones	**Yes**		**Telephones for staff**
Internet Connection	**Yes**		**Varies by employee**

Other

Any hard copy files are stored in fireproof cabinets at the Broadway office. These and other files are converted to digital format and organized appropriately using Google. Current digital files are backed up within Google Drive. Historical records are stored digitally within the Box or Jack cloud systems.

4. Backup Procedures

Backup Procedures		
Asset	**Frequency**	**Comments**
Onsite personnel	**n/a**	**n/a**
Offsite/Remote personnel	**Everyday**	**Onsite personnel back up pertinent files to Google Drive**
Canvas LMS	**Everyday**	**LMS is backed up daily by the vendor.**
DiamondSIS	**Everyday**	**SIS is backed up daily by the vendor.**
Google Drive	**Continuously**	**Google Drive is backed up continuously to Google's storage facility.**

5. Disaster Recovery Procedures

Business operation interruptions are mitigated by the remote nature of the institution and the use of cloud technology in mission critical applications. In the case of an incident which renders the office headquarters incapable of sustaining its operations, BU's cloud-based Learning Management System should not experience a service interruption. All staff are located offsite in remote offices, so business would continue unimpeded.

Emergency Response Procedures

The Technology/Senior Personnel noted in section 2 will be responsible for the steps below.

1. Contact offsite technology personnel.
2. Technology personnel will contact unaffected personnel in the event that they need to take over operations.

Backup Operations Procedures

1. All academic, accounting and financial software, and associated data/databases, can be accessed by staff located in an unaffected area.

Recovery Actions Procedures

1. Senior personnel will determine degree of disaster.
2. Accounting Director will notify insurance companies.
3. Accounting Director will notify all onsite/headquarter vendors, where applicable.

6. Testing the Disaster Recovery Plan

The disaster recovery procedures in section 5 are tested annually.

7. Rebuilding Process

BU maintains adequate insurance to facilitate recovery from a disaster. Senior management will have ample time necessary to find a new facility for headquarters.

DATA BREACH PROCEDURES

Table of Contents

  - DigitalOcean Space
  - DigitalOcean database
  - DigitalOcean server
  - DigitalOcean volume
  - Google Could Platform database

- Fatal Disaster Situation

Amazon Web Services

Unauthorized account access

We don't have access to the IAM console, and we can't evaluate potential damage. When an attacker hacked your account, you need to reset credentials and contact Jordan to review security logs (or block your account if necessary).
Developer accounts are limited, but they can access and manage S3 buckets. It means that files could be downloaded (including sensitive student data) or encrypted (see the ransomware section).

Application

Unauthorized account access

devCamp uses a cookie-based session. It means that changing the password won't prevent a potential attacker from accessing the application.
Use the application console to block access to your user by (1) removing the account or (2) removing the `devcamp_admin` role and all org admin records.
At this point, the attacker could make some actions in the organization dashboard. Keep in mind that devCamp administrators can manage files, download sensitive information like Enrollment Agreements and Government ID, and purge data such as guide videos. Also, devCamp admins have access to Boon via SSO.
Review the following things:

- devCamp admins and organization admins (including the Boon database) as the attacker could modify admin access to the application.
- devCamp and Boon applications logs.
- Automation records in Boon.
- Sent messages in Postmark (for devCamp and Boon) and Twilio (for Boon).

CodeShip

AES Key

It allows to decrypt credentials required to make a deployment (i.e., private SSH key). Follow instructions for "unauthorized access to the server".

Private SSH Key

The private SSH key can leak only on the CodeShip internal security issue. It is used to fetch the code from GitHub.

DigitalOcean unauthorized access

devCamp server account

SSH server access gives wide permissions, including databases, backups, file storage (S3 and DigitalOcean Spaces). In such a situation:

- Shut down the server.
- Revoke access to databases.
- Revoke the authorized key from other servers.
- Setup a new server to "reset" any modifications.
- Review and rotate secrets and credentials (including databases, files storages, email, etc).

Note it might be best to shut down all our servers as soon as possible (but after downloading the secret environment file). This may limit the damaging impact to our services (the attacker may still be able to access other services via downloaded secret environment file). Keep in mind that we can't shut down database services.

Code Tester server account

Code Tester server does not store any sensitive data. However, a potential attacker may replace the output of the application's endpoints stored by devCamp. The outcome is injected as safe HTML on the show guide page, but it can still be used as an attack vector.
Review the following things:

- Check how the attacker logged onto the server (i.e., if captured private SSH key which gives access to other servers).
- Review code submissions in devCamp against modified Code Tester output.

database server

Revoke access to the database, close any opened sessions, and review the impact. If the attacker did not encrypt or modify data yet, it would be enough to rotate the password. If the database has been changed in any way, it will require restoring a backup.

service account

Revoke access (it may be best to remove the user from Bottega account) and review security logs. This kind of break gives access to servers and databases so we may need to perform all other actions from this document.

Gigalixir

service account

Revoke access and rotate secret keys for analytics-app-* and boon-* applications.
Boon shares the secret key with devCamp (due to SSO).
Do the following things:

- Revoke access.
- Rotate secrets for analytics-app-* and boon-* applications (including the secret key shared with devCamp due to SSO).
- Review automation records.
- Review sent messages in Postmark and Twilio.
- Review databases for modifications.

The attacker will gain access to databases via the configuration. We may need to restore database from backups in case of ransomware or modifications.

Google Cloud Platform

database server

The database connection string is stored in applications. The attacker probably compromised the server or PaaS account.
Do the following things beside server/accounts steps:

- Shut down the applications to limit the potential impact (modifying automation actions, etc.).
- Rotate databases passwords.
- Rotate credentials for services from Boon's `services` table.
- Optionally restore database instance from snapshot backup.

Note the production instance hosts databases for Boon and Analytics App applications.

service account

The attacker gain access to databases. Ask Jordan to review security logs and perform steps from the "database server" section.

Heroku

service account

Bottega hosts a lot of applications on Heroku. The most important is probably Enrollment App (leadsnatch). It includes secrets for the following services:

- Stripe,
- Postmark,
- devCamp API client key,
- Calendly.

Do the following things:

- Rotate keys for services.
- Review payment records on Stripe.
- Review logs for devCamp and Enrollment App.

Ransomware

AWS S3

Files stored by devCamp through ActiveStorage are mirrored to DigitalOcean Space. To recover files, ensure the S3 bucket is not a primary backend storage, cleanup the bucket, and schedule mirroring for all blobs.

DigitalOcean Space

Files stored by devCamp through ActiveStorage are mirrored to AWS S3. To recover files, ensure the Space is not a primary backend storage, cleanup the Space, and schedule mirroring for all blobs.
The Space also stored static files. These are currently not mirrored to AWS S3.

DigitalOcean database

The database connection string is stored in devCamp application and it is not possible to connect to it from outside of DigitalOcean resources (see Trusted Sources in database Settings). The attacker probably compromised devCamp server or DigitalOcean admin account.
Do the following things beside server/account steps:

- Shut down the applications to limit the potential impact.
- Rotate database password.
- Restore database from backup.

DigitalOcean server

Do the same steps as for "unauthorized devCamp server account". Note database backups are stored in volume attached to the server. It may not be possible to recever database from a backup file.

DigitalOcean volume

Shut down the server and make sure that database is not encrypted. Currently, the volume attached to the server is the only place where database backups are stored.

Google Could Platform database

Recover snapshot backup via the Google Cloud Platform dashboard.

The database connection string is stored in Analytics App, Boon, and devCamp applications. The attacker probably compromised devCamp server, DigitalOcean admin account, or Gigalixir account.
Do the following things beside server/account steps:

- Shut down the Elixir applications to limit the potential impact.
- Rotate databases passwords.
- Restore database instance from backup.
- Ask Jordan to review GCP security logs.

Fatal Disaster Situation

We are not able to recover the system if the attacker uses ransomware or deletes server, backups volume, and database.

Our Architecture Domains

External services

- Slack https://slack.com
- Heroku https://www.heroku.com
- Gigalixir https://gigalixir.com
- DigitalOcean https://www.digitalocean.com
- Google Cloud Platform https://cloud.google.com
- Amazon Web Services https://aws.amazon.com
- Github https://github.com
- AppSignal https://www.appsignal.com
- Papertrail https://www.papertrail.com
- Codeship https://www.cloudbees.com/products/codeship
- Postmark https://postmarkapp.com
- Pushover https://pushover.net
- Twilio https://www.twilio.com
- Stripe https://stripe.com
- reCAPTCHA https://developers.google.com/recaptcha/
- ICR Evolution https://icr-evolution.mx
- Facebook https://www.facebook.com/business
- Podium https://www.podium.com
- CallHippo https://callhippo.com
- Calendly https://calendly.com

- Google Drive https://www.google.com/drive/
- HubSpot https://www.hubspot.com

Places where we store data

Databases

Analytics App's PostgreSQL database is hosted on Google Cloud Platform. It contains student's activity information: which guides they read, which tutorial videos they watched, how long they interacted with our platform, etc. Students are identified in this DB only by their ID, so without correlating this data with another DB it is not possible to identify users. This database does not contain any personal information. Data contained in this DB is visible to devCamp admins via devCamp's reporting dashboard. Each student can view their activity data in aggregate form via devCamp's UI. Raw DB access is only given to the development team.
Boon's PostgreSQL database is hosted on Google Cloud Platform. It contains personal information on potential, current and past students. That includes emails, phone numbers, names, addresses, etc. Data contained in this DB is visible to devCamp admins via Boon's UI. Raw DB access is only given to the development team.
devCamp's PostgreSQL database is hosted on DigitalOcean. This database contains personal information on potential, current and past students. That includes emails, phone numbers, names, addresses, etc. Data contained in this DB is visible to devCamp admins via devCamp's reporting dashboard. Each student can access and edit their data via the Enrollment App's UI and devCamp's UI. Raw DB access is only given to the development team.
devCamp's Redis database is hosted on DigitalOcean. This database contains no personal information and is used only as a temporary storage needed to perform tasks on the backend. Raw DB access is only given to the development team.
Support App's PostgreSQL database is hosted on Heroku. This database contains personal information on current and past students and teachers. That includes emails, names, IP addresses and database IDs, as well as full chat logs of conversations between students and teachers.

File uploads

All binary data is stored on DigitalOcean Spaces and Amazon Web Services S3. That includes PDFs of enrollment agreements, as well as scans and photos of documents required as part of our enrollment process, like driver's license, passport, energy bill, etc. Data contained in this file storage is visible to devCamp admins via devCamp's reporting dashboard. Each student can access and edit their files via the Enrollment App's UI. Raw file storage access is only given to the development team.

Logs

devCamp application runs on a single server hosted by DigitalOcean. Application and server logs are stored on its local file system and are also mirrored to the Papertrail service. Logs contain user's IP addresses, their browser's user agent strings and URLs of pages they visit. Certain admin actions will also leave logs with more user details like student's email and name. Passwords and auth tokens are filtered out within the app and never end up in logs. Logs are kept for 12 weeks on the server and for 1 year on Papertrail.
Analytics App and Boon applications are hosted on Gigalixir. Application logs are stored in Gigalixir and are also mirrored to the Papertrail service. The only personal information that logs contain are user database IDs and in some cases user emails. Only the last 1500 log lines are kept in Gigalixir. Papertrail keeps 1 year of log history.
Enrollment App and Partner Page applications are hosted on Heroku. Application logs are stored in Heroku and are also mirrored to the Papertrail service. Logs contain user's IP addresses, their database IDs and emails. Only the last 1500 log lines are kept in Heroku. Papertrail keeps 1 year of log history.
Code Tester application runs on a single server hosted by DigitalOcean. Application and server logs are stored on its local file system and are also mirrored to the Papertrail service. Logs contain no user information. Logs are kept for 12 weeks on the server and for 1 year on Papertrail.
Support App's applications are hosted on Heroku. Application logs are stored in Heroku. Logs contain user's IP addresses, their database IDs, emails and names. Only the last 1500 log lines are kept in Heroku.

Backups

Backups of Analytics App and Boon databases are made automatically by Google Cloud Platform, once a day and stored for 7 days. Only the development team has access to those backups via GCP UI.
Backups of devCamp's PostgreSQL database are made automatically by DigitalOcean, once a day and stored for 7 days. Only the development team has access to those backups via DO UI.
Additional backups of devCamp's PostgreSQL database are made via a custom backup script, once a day and stored for 180 days on a separate disk volume. Only the development team has access to those backups via server SSH. The additional backups are encrypted using the key stored on the production server.
devCamp's Redis database is not backed up at all, as it only contains ephemeral data.
Backups of Support App's PostgreSQL database are made automatically by Heroku, with the ability to rollback any changes made within the last 4 days. Only the development team has access to those backups via Heroku UI.

External services

AppSignal is a service that stores information about errors and performance of our applications. Error and performance samples may contain some private information like user database ID, user-agent string of their browser and their IP address. In some rare cases error details may contain other user information like email, names, addresses, etc. Data in AppSignal is stored for 30 days.
Google Drive and HubSpot contain information on leads (potential students): names, emails, phone numbers, etc. Only the sales team has access to those services.

Access points

Access to Google Cloud Platform UI allows downloading Analytics App and Boon databases, as well as removing all data, including backups.
Access to DigitalOcean UI allows downloading devCamp database, as well as removing all data, including backups. It also allows full access to file storage on DO Spaces, allowing to download and remove all files.
Access to Gigalixir UI allows downloading Analytics App and Boon databases, as well as removing all data, but *not* backups.
Access to devCamp server via SSH allows full access to devCamp's database, Boon's database and S3 and DO Spaces file storages. This access allows downloading and removing all data, including devCamp's DB backups, but *not* Boon's DB backups.
Access to Heroku UI allows access to devCamp's API that provides capability to download and clear all students information from devCamp, but *not* backups. This can be achieved through utilization of the API key found in Enrollment App's configuration or API key found in Support App's database. It also allows downloading Support App database, as well as removing all data.
Access to Github UI would allow arbitrary code to be deployed to the devCamp server, Enrollment App, Partner Page and Support App, thereby allowing full access to devCamp's database, Boon's database, Support App's database and S3 and DO Spaces file storages. This access allows downloading and removing all data, including devCamp's DB backups, but *not* Boon's DB or Support App's DB backups.
Access to Papertrail UI allows access to all logs stored in that service (see *Logs* section above for details), as well as removing all data, including backups.
Access to Amazon Web Services UI allows full access to file storage on S3, allowing to download and remove all files.
Access to Codeship UI allows access to the devCamp server, which in turn allows access to databases and file storage, as was listed above.