DATABREW STANDARD OPERATING PROCEDURES FOR DATA MANAGEMENT

PROCESSES AND PROCEDURES FOR IT, ANALYSIS AND DATA MANAGEMENT

REVISION DATE: 07/01/2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Databrew is a data science consulting company that offers customized solutions and approaches to data collection, storage, management, and analytical needs for our clients.

We are committed to and responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on our systems. Thus, all employees interacting with our company's information assets have a responsibility to ensure the security of those assets.

Databrew also relies on several technological assets for our business endeavours and ensuring the physical and logical security of these devices is of utmost importance.

This Standard Operating Procedures Manual outlines the purpose, scope, and procedures for various controls put in place to ensure the smooth operation of the company's hard- and software resources. All Databrew employees and contractors must be trained, equipped, and periodically reminded on how to use information and associated infrastructure securely.

1. SYSTEM MAINTENANCE

1.1 Purpose

The purpose of this procedure is to describe the activities involved in ensuring that Databrew's systems and data are maintained in an operational state.

1.2 Scope

This procedure applies to information technology systems, servers, and software supporting Databrew's activities.

1.3 Definitions

- "System" refers to both the physical assets (computers, servers, tablets, etc.) as well as the code-base and environment on which those assets run.
- "Data management" refers to all aspects of the data lifecycle: collection, processing, storage, backups, etc.
- "Third party" refers to entities that are not directly under DataBrew's authority or sponsorship. Importantly, for the purposes of this document, "third party" excludes those web services which are of common use in the tech industry (Amazon Web Services, Google Cloud, etc.).

1.4 Procedure

Routine Maintenance

Databrew management shall perform maintenance of operating systems in accordance with approved agency information technology security requirements. They should consider the following issues when supporting operating systems:

1. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.
2. Periodic maintenance improves the performance of operating systems (e.g., hard drive defragmentation).
3. If maintenance support is provided by a third party, nondisclosure statements shall be signed by authorized representatives of the third party before any maintenance support is performed.

Hardware/Software Upgrades

Hardware (computers, tablets, etc.) will be upgraded on an as needed basis. Databrew management will determine the issue and necessary hardware upgrade, ensure all data is properly backed up, make the replacement, and document any upgrades/purchases made.

A software upgrade is a new version of the software that offers a significant change or major improvement over the current version and should be conducted when available under the direction of Databrew management. In the case that a software upgrade requires the purchase of the new version of the software, the purchase must be approved by Databrew management.

Operating System Upgrades

Operating system (OS) upgrades can make important changes to your system in functionality, user interface, and general appearance over the previous version. Databrew management will determine when OS upgrades are necessary and make the necessary upgrades to all devices.

Last updated: 2019-07-01
Approved by: Xing Chiu

2. PHYSICAL SECURITY

2.1 Purpose
Physical damage or destruction to technological devices can impair the confidentiality, integrity, and availability of information. The purpose of this procedure is to describe Databrew's application of physical security measures to protect portable technology and devices.

2.2 Scope
This procedure applies to all Databrew employees and contractors.

2.3 Definitions
Physical Security: Protection of hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution.

2.4 Procedure
The security and safety of all company portable technology, including but not limited to laptops, tablets, monitors, and mobile phones will be the responsibility of the employee who has been issued with the device.

Databrew management will instruct all employees and contractors how to properly handle company equipment.

Each employee is required to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

Laptops and other portable technology devices should be transported with proper packaging and never left unattended in public.

Care needs to be taken to ensure that classified and protected information and valuable assets (e.g., laptops) are properly safeguarded when users are away from their workstations for any length of time.

In the event of loss or damage, Databrew will assess the security measures undertaken to determine if the employee will be required to reimburse the company for the loss or damage.

Last updated: 2019-07-01
Approved by: Xing Chiu

3. LOGICAL SECURITY

3.1 Purpose
The purpose of this procedure is to describe Databrew's appropriate logical security measures necessary to protect data and users.

3.2 Scope
This procedure applies to all systems, employees and contractors at Databrew.

3.3 Definitions
Firewall: A network device which uses rules and policies to manage the data traffic which is allowed in and out of the company network.

Logical Security: Software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

3.4 Procedure
Logical security consists of software safeguards for Databrew's systems, including user identification and password access, authentication, access rights, and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in our network.

Firewalls
Firewalls protect a system from access or intrusion by outside or untrusted systems or users, especially malicious hackers. A firewall should also keep a log of any such attempts. For greater security, a personal firewall or a system-based intrusion-detection agent should be active in all devices used by Databrew employees and contractors.

Network Access
Databrew management should secure access to computer networks through multiple layers of access controls by doing the following:

- Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone
- Implementing appropriate controls over wired and wireless networks

Account Management
Databrew management will manage accounts by:

- Assigning users and devices the access required to perform required functions
- Updating access rights based on personnel or system changes
- Reviewing users' access rights at an appropriate frequency based on the risk to the application or system
- Designing appropriate acceptable-use policies and requiring users to agree to them
- Controlling privileged access
- Changing or disabling default user accounts and passwords

Users leaving the company will have their network access rights removed upon termination of employment. All company accounts will be disabled.

External contractors's physical and logical access to any system will be granted based on least privilege. When establishing accounts, standard security principles of "least privilege" to perform a function must always be used, where administratively feasible. Access privileges should be limited to those that the user has a genuine need for to complete job responsibilities and functions.

Password Management

Initial passwords are created by Databrew management users are asked to change their password upon initial login. Accounts on all systems will use non-shared, unique passwords.

Last updated: 2019-07-01
Approved by: Xing Chiu

4. INCIDENT AND PROBLEM MANAGEMENT

4.1 Purpose
The purpose of this procedure is to define the requirements to ensure that any unplanned Information Technology incident that could impact product quality and data integrity is addressed in order to minimize the disruption of operational activities.

4.2 Scope
This procedure applies to operational systems in use by Databrew.

4.3 Definitions
"Incident" or "problem" refers to any event which is outside of the scope of operations and could compromise, in any way, the system's security, the user's privacy, or the data's integrity.

4.4 Procedure

1. Where possible, Databrew will take preventative measures to stop problems from occurring and minimize the impact of incidents that do occur by addressing identified problems as quickly as possible.
2. Problems and incidents with a priority of urgent or high must be reported within two hours of detection to contain the issue, and if possible, prevent any further impact.
3. Databrew will conduct investigations into problems and incidents with priorities of urgent or high to determine the root cause of the issues, to remediate the issues and return to a normal situation in a timely manner.
4. Databrew will communicate with internal and external stakeholders impacted by the problem or incident.
5. Employees, contractors, and partners will receive explicit encouragement in sharing problems
6. In the event of any incident that could have potential privacy implications for end-users, both (a) the relevant regulatory authorities will be contacted as well as (b) the end-users themselves, with a full description of the nature of the incident, remediative steps, and potential implications

Last updated: 2019-07-01
Approved by: Xing Chiu

5. SYSTEM CHANGE CONTROL

5.1 Purpose
The purpose of this procedure is to define a formal process for change management that will ensure that system changes are implemented in a controlled fashion. The procedure will also describe the framework for proposing, reviewing, and approving changes to a system.

5.2 Scope
This procedure applies to changes intended for Databrew's validated information technology systems that are in operational use.

5.3 Definitions
Change: Any modification that must be planned for, evaluated, tested, documented, scheduled, and authorised prior to use.

5.4 Procedure
Changes to Databrew's business processes and information systems that affect information security must be controlled. All changes to the company's services and systems environment, including provisioning and de-provisioning of assets and configuration changes must be authorized by Databrew's management team in order to ensure changes are introduced to the environment in a controlled manner.

Application and system control considerations for introducing changes to Databrew's IT environment before implementation should include the following:

- Clearly defining requirements for changes.
- Restricting changes to authorized users.
- Reviewing the impact that changes have on security controls.
- Identifying all system components affected by the changes.
- Developing test scripts and implementation plans.
- Performing necessary tests of all changes to the environment (e.g., systems testing, integration testing, functional testing, user acceptance testing, and security testing).
- Defining rollback procedures in the event of unintended or negative consequences with the introduced changes.
- Ensuring the application or system owner has authorized changes in advance.
- Maintaining strict version control of all software updates.
- Validating that new hardware complies with institution policies.
- Ensuring network devices are properly configured and function appropriately within the environment.
- Maintaining an audit trail of all changes.

Last updated: 2019-07-01
Approved by: Xing Chiu

6. CONFIGURATION MANAGEMENT

6.1 Purpose
The purpose of this procedure is to ensure that all updates to baseline items are controlled and traceable.

6.2 Scope
This procedure applies to deploying systems and ensuring compatibility, homogeneity, and reproducibility of Databrew's IT infrastructure.

6.3 Definitions
"Configuration" refers to the physical or virtual arrangements, combinations, and options, as well as versioning.

6.4 Procedure
Configurations can be divided into two types: (1) those which are cross-project and general to Databrew operations as a whole (such as the "databrew" R package, https://github.com/databrew/databrew), and (2) those which are specific to projects (such as the Bohemia IT administrator guide, http://databrew.cc/instructions/bohemiaadmin.pdf). Configurations should employ best practices (particularly in terms of privacy and security), be fully documented, and rely on version-controlled code. All code and documentation should undergo at least one round of "peer review" via pull requests (for code review) and commented examination (for written text).

Last updated: 2019-07-01
Approved by: Xing Chiu

7. DISASTER RECOVERY

7.1 Purpose
The purpose of this procedure is to outline how Databrew should respond in the event of a disaster.

7.2 Scope
This procedure applies to the Information Technology infrastructure at Databrew.

7.3 Definitions
Disaster: An unplanned event that causes a system to be inoperable, unable to provide critical business functions, and potentially results in a loss of data.

7.4 Procedure
In the case of a disaster, the employee who identifies disaster will notify Databrew management, who will:

- Determine the nature and degree of disaster
- Isolate the compromised system(s)
- Search for additional compromised systems
- Implement proper application recovery plan dependent on the nature and extent of disaster
- Notify clients in the case of any delays with project timelines
- Contact hardware and software vendors, as necessary
- Restore systems, programs, and data to a known good state

Last updated: 2019-07-01
Approved by: Xing Chiu

8. ELECTRONIC SIGNATURE

8.1 Purpose

The purpose of this procedure is to establish a process for obtaining and tracking electronic signatures, as well as establishes when an electronic signature may replace a written signature.

8.2 Scope

This procedure applies to all Databrew employees and consultants, and governs all uses of electronic signatures and electronic records that are generated as part of the company's activities. This procedure may also apply to additional activities which may include, but not be limited to, the generation of electronic communications, transactions, contracts and any other document or record that requires a signature.

8.3 Definitions

Digital Signature: An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

8.4 Procedure

1. To facilitate the use of electronic signatures:
    a. Databrew shall, through its normal procurement processes, acquire software to facilitate the use of electronic signatures.
    b. Each person authorized to sign contracts on behalf of Databrew shall be issued a license for the electronic signature software.
2. The system used to sign electronic contracts shall capture the document at the time of signature and shall securely store it so that the signed version may be retrieved in the event of a dispute.
3. The electronic signature software shall require a separate and distinct action for each signature.

9. BACKUP AND RESTORATION

9.1 Purpose
The purpose of this procedure is to describe the backup and restore process for all systems/servers used by Databrew.

9.2 Scope
This procedure applies to backup and restore processes managed by all employees at Databrew.

9.3 Definitions
Backup: A point in time copy of a file(s) that resides on a computer storage medium. Backups can be overwritten.
Full Backup: All files are copied, regardless of their creation date or time of last access.
Incremental Backup: Only files modified since the last full or incremental backup are copied.

9.4 Procedure
Backup Process
Backup copies of data, information, software, and system images must be made, secured, and be available for recovery. It is the responsibility of Databrew to ensure that data backups are conducted on a regular schedule and the backed up data is kept in a secure location.

Servers (both virtual and physical) such as operating systems and associated applications (i.e., databases, web server applications, etc.) for all Windows, Linux, and other types of operating systems will be backed up.

Full backups, which capture all files selected for backup, will be completed on a daily basis. Depending on the volume of data and frequency, full backups can require a large storage capacity and a significant amount of time to record the information. In cases where much of the data does not change from backup to backup, other options may be considered. Incremental backups of new data will be performed on a daily basis.

Restoration Process
The restoration process will consist of the following tasks:

- Replace or repair damaged equipment
- Upgrade damaged equipment
- Reconfigure replaced/damaged/upgraded equipment
- Set up for processing at alternate site
- Retrieve backup data, software, licenses, etc. from external storage
- Contact vendors for repairs or replacement of hardware and software
- Test equipment and software prior to resuming normal processing
- Document all recovery actions taken