Harvest Trends

Data Security Policy

V3

Updated: 6/08/2017

Contents

Introduction

This document describes the policies and procedures that must be followed by employees of Harvest Trends to ensure the robust protection of client data in the secure environment at Oracle Corporation.

Context

Harvest Trends chose to invest in hosting the application software and client data at Oracle Corporation. Employees will not install application software components or databases outside of the secure environment at Oracle Corporation.

This decision to invest in Oracle Corporation was made because of the following:

- Oracle Corporation has the resources to invest in, and maintain, a high degree of data security including robust physical security at the data center(s), network resilience to attacks, operating system patches, and data integrity.
- Oracle Corporation provides secure back-up and restore, and disaster recovery via dual locations for the production data and back-up data.
- The Oracle Cloud environment implements robust password standards and a 90-day password reset policy.

Please refer to the latest Oracle Cloud Security Whitepaper for full details on the investment that Oracle Corporation makes in a robust approach to application and data security.

Key Principles

- Client data should be securely uploaded to the secure Oracle environment.
- Client data should remain within the secure Oracle environment.
- Client users should not be able to download data from the Power Host application.
- Client reporting should be via the secure Oracle Business Intelligence solution at Oracle.
- Employees will only use a Harvest Trends computer on a secure network.

Employee Distribution

Employees are required to sign the addendum that they have read and understood this document, and understand that their continued employment is contingent on their adherence to this policy.

Managers are required to obtain signed copies from their direct reports and file them. New employees must sign before they are given system access of any kind including email. Current employees must sign any revised edition within 2 working days of issuance.

Change Control

Changes to this document can only be made by the CEO who is the acting Chief Security Officer (CSO).

Contractual Agreement

The reputation of Harvest Trends, and our clients, depend upon the employees adhering to these policies and protecting the integrity of client data.

In addition, Harvest Trends signs a contract with clients that includes terms and conditions related to Confidential Information.

Employees will be familiar with the contractual terms between Harvest Trends and the Client. Employees will act in a manner consistent with the letter and intent of these contractual terms

"5. CONFIDENTIALITY

5.1. Confidentiality. **"Confidential Information"** means any nonpublic information (written, oral or electronic) disclosed by one party to the other party and shall be deemed to include, without limitation, the following information of the respective parties: (a) the e-mail addresses and names of Client contacts, business plans, technical data, product ideas, personnel, contracts and financial information; (b) patents, trade secrets, techniques, processes, know-how, business methodologies, schematics, employee suggestions, development tools and processes, computer printouts, computer programs, design drawings and manuals, and improvements; (c) information about costs, profits, markets and sales; (d) plans for future development and new product concepts; (e) all documents, books, papers, drawings, models sketches, and other data of any kind and description, including electronic data recorded or retrieved by any means, that have been or will be disclosed, as well as written or oral instructions or comments; (f) any Client Data or information stored on Harvest Trends equipment.

5.2. Non-Disclosure. Each party agrees not to use, disclose, sell, license, publish, reproduce or otherwise make available the Confidential Information of the other party except and only to the extent necessary to perform their respective obligations under this Agreement. Each party agrees to secure and protect the other party's Confidential Information in a manner consistent with the maintenance of such party's own confidential and proprietary information and to take appropriate action by instruction or agreement with its employees, consultants or other agents who are permitted access to the other party's Confidential Information to satisfy its obligations under this Section.

5.3 Nondisclosure Obligation Excused in Certain Situations. The obligation to treat information as Confidential Information shall not apply to information which: (a) is publicly available through no action of the receiving party; (b) shall have been in the receiving party's possession independent of its relationship with the disclosing party; (c) shall have been developed by or become known to the receiving party without access to any of the disclosing party's Confidential Information and outside the scope of any agreement with disclosing party; or (d) shall be obtained rightfully from third parties not bound by an obligation of confidentiality."

Client Responsibility

"4. CLIENT RESPONSIBILITY

4.1. Password Security. Client shall be responsible for undertaking measures to ensure the confidentiality of Client passwords. If a Client password is lost, stolen or otherwise compromised, Client shall promptly notify Harvest Trends, whereupon Harvest Trends shall issue a replacement password. "

Upload of Data

It is a fact that some casino clients are less security conscious than others but Harvest Trends employees are required to treat the data from all clients with equal care and consideration:

- Employees must dissuade clients from sending patron data via email. Any breach of security because a client sends data via email will reflect on Harvest Trends and not just on the client.
- Employees must emphasize to clients that Citrix Sharefile is available for one-off file upload and for automated daily upload. Sharefile has been selected because it is easy for any client to use for manual or automated uploads.
- If a client sends patron data via email, the employee should reply with a reminder about Sharefile and with instructions on how to upload.
- If a client contact is a repeat offender, the employee should notify the CEO who will speak to client management about the need to use Sharefile.

The sales team should encourage the use of a consultant to assist the client with uploading the data in an automated secure fashion, including the now proven option of the client transferring data directly into the Oracle database.

Extraction of Data

There is no Harvest Trends business practice that requires extraction of data from the secure Oracle environment.

There have been, and will occasionally be, scenarios in which the client requests the extraction of a subset of data:

- The request must be approved or initiated by a Manager at the client casino. Data will never be extracted for an end-user.
- In the event that the client requests extraction of data from the secure Oracle environment, then this will be done in response to:
    1. An approved ZenDesk support ticket opened by the client (e.g. an audit history for the results and actions of a specific Host that the Client is researching)
    2. A pre-approved client business process that is documented in an email from the client manager (e.g. a quarterly audit of goals). Any recurring business request should be implemented in the secure Oracle Business Intelligence solution.
- Extracted data will be loaded to Sharefile for the client to download; it will not be emailed to the client.
- Employees will ensure that extracted data is not retained on the local hard-drive e.g. in the Download folder.
- Employees will only use their Harvest Trends computer and on a secure network.

Employees will be terminated with cause for extracting client data from the secure Oracle environment without a pre-approved request from a client.

Modification of Data

There have been, and will be, scenarios where the client requests modification of production ratings e.g. run-away slot ratings that resulted in inaccurate Theo. In the event that the Client requests a limited change to production ratings, access will be pre-approved by the CSO inside the ticket.

Reproducing Production Issues

When a client reports an issue, the team will try to reproduce the problem inside the development environment with the fake 'Sandy Palace' dataset.

In the event that the Client is experiencing a production issue that cannot be reproduced in the development environment, then these are the appropriate options:

- If the problem with the front-end of Power Host, the HelpDesk will arrange a Join.me session with the client user who will demonstrate the problem via a webinar. The employee will not request the password of the client user.
- If the problem is with the back-end data, the DBA access for trouble-shooting the issue will be pre-approved by the CSO inside the ticket.

Configuration of Power Host

During the start-up phase, the assigned employee(s) will require access to the client's production environment to pre-configure and test Power Host including: database, custom SQL for client business rules, data transformation logic, configuration of options for Player Development, coding of goals, and user access. During this configuration phase, the client will be asked to upload sample data.

When the start-up phase is complete, the CSO will change the password for the usernames defined as the Production Username(s) and the HelpDesk will inform the client that their production environment is ready for production data.

Production Username(s)

The Production Usernames are the user names for automation that transforms and processes the client data each day:

- Transform client data
- Analyze host activity
- Calculate host goals, classifications, recommendations, tasks etc.
- Initiate client reporting via Oracle Business Intelligence

The password(s) for Production Username(s) will be known only to the CSO. The Company Secretary will have the ability to access passwords in the event that something happens to the CSO. The Client should expect to see the Production Username(s) in the transaction logging as the automation runs each day.

Change Control for Development

Harvest Trends will continue to enhance the application and data structures to add useful features and in response to client requests.

Changes to Database

A DBA will not initiate a change to a database without the existence of an approved open ticket for a new feature, client enhancement, or problem resolution.

A DBA will add a comment to the Version History of the SQL code with their name, date, ticket number, and description of the change. A DBA will add the date and ticket number to every line that is added, deleted or modified. Deletions will be commented out.

A change to the database will not be deployed to Production without review by Quality Assurance (QA). A DBA will use their own username and credentials to make such a change.

If a client has been identified as security-conscious in their client profile, then the assigned QA member will notify the HelpDesk who will issue a Configuration Change notice to the client.

Changes to Application

A developer will not initiate a change to the application without the existence of an approved open ticket for a new feature, client enhancement, or problem resolution.

A change to the application will not be deployed to Production without sign-off from Quality Assurance (QA). QA will use change control to identify all changes at the file level.

If a client has been identified as security-conscious in their client profile, then the assigned QA member will notify the HelpDesk who will issue a Configuration Change notice to the client.

Test data

Developers and DBAs require test data to make changes, and the QA team requires test data to test changes. Production data will not be used, or extracted to test systems, to create test data. The fake ‘Sandy Palace’ dataset is available.

** Please note. Some clients will be marked as Security Conscious in their profile and will receive a Configuration Change notice. But, regardless of the sophistication of the client with regard to data security, Harvest Trends will adhere to the policies in this document to protect the integrity of player data for all clients.

Auditing

Automated audit trails are used at Harvest Trends for a number of reasons:

- Deter employees from inappropriate actions (e.g. provide an audit trail of access to systems and data, and enable management to tie such actions to pre-approved tickets)
- Deter client users from inappropriate actions (e.g. provide an audit trail of the creation/deletion of end-users)
- Enable a client to monitor non-client access to their patron data (e.g. via transaction logging on Select statements and on Create Session requests.). A transaction log will be replicated to a client-accessible table in the client schema (UNIFIED_AUDIT_TRAIL)
- Alert management to suspicious activity via triggered reporting on audit logs.

In addition to the automated audit trails, employees are required to update the ticketing system to explain their activities. It is grounds for termination without cause to not maintain this description of the business rationale and the steps taken.

Retention

The software components generate a variety of log and diagnostic files for access to systems, applications and data. Managing the identification and removal of these files to avoid running out of file storage space is an important administrative task.

These are the retention rules:

- Audit trails within Power Host are small and not to be deleted unless the service is terminated by the client.
- Audit trails for data access are not to be deleted for three years or when the service is terminated by the client.
- Logs and diagnostic files for application and database software can be removed monthly since these are not used for audit purposes.

Per the contract, client data is purged when the service is terminated by the client.

Addendum

My name is:

I have read and understood this revised security policy for Power Host.

If I had any questions or concerns then I have asked those questions and received answers from my manager. I no longer have any confusion regarding the content of this security policy and my role and responsibility in the context of protecting data.

I understand that the business model at Harvest Trends involves protecting client data. I appreciate that any breach in data security could damage the brand and finances of Harvest Trends.

I understand that my continued employment at Harvest Trends is contingent on my adherence to this policy.

I understand that my actions, regardless of the intention behind my actions, are grounds for disciplinary action, including termination with cause.

I understand that if I breach this policy on the recommendation from, or instruction of, my manager(s) then I will still be terminated with cause and so will my manager(s).

I understand that I will be required to review and sign all future versions of this security policy for Power Host and that, if I refuse to sign, then I can be terminated with cause.

I understand that this security policy applies to all clients of Harvest Trends regardless of their degree of security-consciousness, or whether they have been identified as security-conscious in their profile. I understand that the only difference is that clients identified as security-conscious have requested additional visibility into change control.

Signed:

Dated:

Manager Name: