2Cana Policy for HiP Hosting Security			
ISSUED BY	DBA Team and Systems Team	Date	2018/02/21
APPROVED BY	Management Forum		

Revision History

Date	Author	Details
2018/02/21	Siphiwe Memela	Original
2019/10/31	Raymond Diack	Physical and OS security aspects updated

Purpose

This policy is approved by 2Cana Risk Management and sets out the HiP Hosting security standards and features available for hosted HiP systems, as well as the logical and physical safeguards in place to protect the system.

These are designed to minimize the potential exposure to 2Cana Solutions and our clients from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of these systems, and in many respects may be customized to meet the security requirements of the client's environment.

Policy Scope

This policy applies to all hosted HiP systems and employees of 2Cana Solutions responsible for administering them, as well as Vendors, Contractors, 3rd Parties and any others involved with 2Cana Solutions in relation to the HiP system. All HiP systems operated by 2Cana Solutions must comply with this policy in alignment with the rules of the client's environment.

Violation and Enforcement of Policy

If it is suspected that this policy is not being followed, report the incident to the Head of 2Cana Systems and IT Risk Management. Any exceptions to this policy must be approved in advance by the Head of 2Cana Systems and IT Risk Management. Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of the Company.

HiP Security Standards

Application Security

HiP is an Oracle application, thus at the database user level, standard Oracle security rules apply. At the application level, role separation is implemented by each client's HR department. This allows fine-grained control of what application modules each user has access to, and by implication, which data the end user has access to.

Out of the box the database security can be customized to fit your environment's requirements. End user accounts are created at the database layer and rules regarding complexity, lifetime/expiry, session lifetime, maximum connections per user are all configurable from the database layer according to your environment's rules. Therefore, when a user logs in to HiP they are logging in to the database. Likewise, a locked database account locks access to HiP.

Database Security

As explained above, fully customizable to the environment's security requirements. Passwords are by default stored encrypted by Oracle in the database. To ensure data privacy in shared environments, internal private databases are used to separate user populations sharing a single hosted database.

Web Portal Security (network security)

Since web portals are Internet-facing, the servers running them are protected from being directly exposed. The application servers reside behind a firewall and access to them is indirect, i.e. via a reverse proxy server with specific rules configured.

Password Security

- Web Portal passwords are stored hashed and thus cannot be easily decrypted without knowledge of keys involved.
- The web portal uses one time pins (OTP), SMS or email for verification purposes during a user-initiated password reset process.
- The HiP application has designated-administrator facilities for use in resetting or unlocking user passwords within the Hip Application (excl. Web Portals). This is covered during training.
- Password history, complexity, lifetime are defined according to the needs of the environment and generally differ between different HiP installations.

- Passwords are by default encrypted during transmission between the middleware and the Oracle database.

Operating System Security

- All system account passwords are securely stored in encrypted password safes, which are accessible only to the relevant teams involved.
- Passwords are split into separate safes for each technical team to ensure that access levels align with duties and that the principle of least privilege is followed.
- Only authorized users can log onto the servers. Active Directory authentication is used.
- Security logs are reviewed on a regular basis to detect any unauthorized access attempts. We are planning on implementing a SIEM (Security Information and Event Management) system to collate security events from all systems into one searchable database for monitoring and audit purposes.

Physical Security

- Access to the physical equipment at the production and DR hosting facilities is strictly controlled using both biometric access into the facility, and key-based access to the cabinets.
- Cabinets are kept locked during normal operations, and the keys are only made available to authorized personnel that have logged an access ticket. The ability to log access tickets is restricted to authorized users only.
- Access onto the premises at the hosting facility is only granted on presentation of a valid access ticket which is only valid for a specific time period.
- All access is logged and reported on, on a monthly basis

Change Management

A Change Management process is critical, ensuring that changes are made in a logical, orderly manner. Individuals responsible for administering HiP systems must always adhere to the 2Cana Change Management process.