Information Technology Department
Policy Document

Access Control Policy

Document Summary

Item	Details
Organization	PVR Ltd
Document Name	Access Control Policy
Classification	Public
Compliance Reference	

Document Revision History

Date	Version	Prepared By
18th April 2016	1.0	Gaurav Amar

Document Review History

Reviewed By	Version	Date	Signature
Mr. Rajat Tyagi (CIO)	1.0	21st April 2016	

1. Scope

This policy applies to all assets of PVR Ltd. The policy specifies how to manage access control to PVR Ltd critical assets

2. Policy

1. The Organization controls access to information on the basis of business and security requirements.

2. Access control rules and rights to applications, expressed in standard user profiles, for each user/group of users are clearly stated, together with the business requirements met by the controls.

3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

4. Access to critical assets should be authenticated, which includes individual users, applications, and administrators.

5. Users should be authenticated through an automated access control system using unique ID and additional authentication (for example, a password) for access to the cardholder environment. Group or shared user-ids should not be used for any of the devices.
   The Users are restricted access to critical assets based on need to know basis and should be set to "deny all" unless specifically allowed.

6. Password Policy should be as follows:
   - Set first-time passwords to a unique value for each user and change immediately after the first use
   - Change user passwords at least every 60 days
   - Require a minimum password length of at least seven characters
   - Use passwords containing both numeric and alphabetic characters Password History to be maintained for at least last 3 passwords.
   - Limit repeated access attempts by locking out the user ID after not more than six attempts
   - Set the lockout duration to thirty minutes or until administrator enables the user ID
   - Session-time out must be set to 30 mins.

7. The access rights to each application should take into account:

   - The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the [systems and] network(s),
   - The "need to know" principle (i.e. access is granted at the minimum level necessary for the role),
   - "Everything is generally forbidden unless expressly permitted",
   - Prohibit user initiated changes to user permissions,
   - Enforcing rules that require specific permission before enactment,
   - Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

8. The Organization has standard user access rights for common roles in the Organization based on the document e.g. Email/Domain Creation form exists within **PVR Ltd.**

9. Management of access rights across the network(s) is done by the Systems Administrator and reviewed by the Information Security Team in line with application access, email/domain creation forms exists within **PVR Ltd**

10. Shared access to organization resources by sharing passwords or group passwords are explicitly prohibited.

11. User access requests, authorization and administration roles should be segregated.

12. User access/revoke requests are subject to formal authorization from relevant stake holder on an email

13. Access are periodically reviewed by IT admins at cinemas for Vista. For other applications the change review is conducted by relevant stake holders.

The IT Team is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy was approved by Chief Information Officer and is issued on a version controlled basis under his/her signature

Signature: Nayat Lyogi

Date: 21/4/16