blueprism®

Robotic Process Automation Software

Blue Prism

SECURITY POLICY AND PROCEDURES

Version: 2.0

For more information please contact:

info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 7577476

www.blueprism.com

Revision History

Date	Revision	Author	Description
20/9/2019	2.0	Mike Lawrence	Updated for ROM 2.0

Contents

Blue Prism Limited, Centrix House, Crow Lane East, Newton-le-Willows, WA12 9UY, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

1. Introduction

This document outlines the security policy and procedures that supports the Blue Prism Robotic Process Automation software platform, which is robust, highly scalable, powerful and flexible, designed from first principles to provide organisations with a business owned and IT supported Digital Workforce.

Any organisation wishing to utilise the Blue Prism application for process automation should complete this document with the assistance of the relevant departments (Blue Prism team, business process owners, security department, access control department, IS department).

Once completed this document should outline the approved procedures for operating within the Robotic Operating Framework – a practical modus operandi which both respects and supports the security principles on which the security policy is based.

Where possible, Blue Prism have identified and described within this document some recommended security procedures based on previous implementations of the product. These recommendations are intended to inform rather than dictate the final decisions made herein.

2. Initial Blue Prism Setup Recommendations

Blue Prism recommends the following settings are immediately after the Blue Prism application is installed. These are initial settings for the development environment only, the UAT or live environments should not be used without the completion of this document and its full adherence.

- *Development database – development should initially take place in a low priority development database, even a local instance of Microsoft SQL Server express. No sensitive client information should ever be stored in the development database and session logs should be deleted daily to ensure no data is held.*
- *User privileges – we recommend that from the start as much dual control is put in place as possible. A system administrator role user should be allocated as soon as possible to monitor the use of user creation etc.*
- *No anonymous users – the initial set up admin user created for a new Blue Prism installation should be deleted once 'real' users have been created.*
- *Password complexity – Initial development passwords should be immediately set up to require a minimum of 8 characters, a variety of characters (i.e. numeric), and no re-use of the last 12 passwords. Passwords should be set to expire within 4 weeks.*
- *Credentials – credentials, possibly, may not be used is during the initial days of the configuration period. This is when the Process Developer will begin to model the target application in Blue Prism and invariably this will involve automating the 'launch' and 'log in' procedure. As the Process Developer is also likely to require the ability to log in manually, the implementation of Credentials may be temporarily delayed until these early steps have been completed. Thereafter Credentials will be used as normal. Note: If Data Gateways are to be used a credential will have to be created regardless.*

3. Blue Prism Application

This section of the security policy document relates to ensuring that the Blue Prism application is used in a secure and appropriate manner, and users of Blue Prism only have access to the parts of the application to which permission has been agreed in accordance to their role.

3.1. Role Definitions

The following user roles are available with the Blue Prism product:

Role	Description
Developer	A user who creates and/or amends Blue Prism processes and objects
Lead Developer	A user responsible for supporting the creation and evolution of the delivery framework, mentoring other process developers and delivering automated processes
Solution Designer	A user who designs automated solutions based on Blue Prism best practices and principles
Release Manager	A user who has privileges to move some or all of a Blue Prism developments (i.e. processes, work queues etc.) from and to an environment
System Manager	The System Manager has the authority to approve users and their privileges and authorise emergency changes, supporting the environment feasibility
Process Controller	A user responsible for ensuring that processes run correctly each day. This may involve, starting and stopping processes, monitoring performance, inspecting queue activity, etc.
Support Analyst	A user who provides support in detail and test Blue Prism process in either Process Studio and/or Control Room
System Administrator	A user who has privileges within the Blue Prism software. These privileges may only be exercised within the procedural guidelines established in the accompanying framework documents and under the authorisation of the System Manager. The primary role of the System Administrator is to manage the privileges of other users, granting and revoking access to various environments as and when required
Runtime Resource	The user role used by a resource at run time

3.2. User Role Specifics

- *<within this section the product access given to each role within each environment (development, UAT, production) should be outlined.*
- *<within this section any required division of privileges and responsibilities between roles must be defined>*
- *Please reference your* ***Blue Prism Logical Access Model (LAM)*** *framework that should accompany this document.*

Blue Prism Recommendations

As a matter of principle, each user should be given the minimum level of privileges necessary to perform their daily duties. In particular:

- *All editing of processes and objects is prohibited in the production and UAT environments. No users have permission to modify processes or business objects in the production environment.*

- *The operational teams who start/stop processes from day to day may use Control Room in order to do so; they may not edit processes/objects or make system changes. They may view reports, view (or otherwise analyse) process diagrams, access statistics, read process logs, etc.*
- *Delivery managers (and other users with an analytical role) do not have permission to run processes. They merely have access to the required reporting and (read only) process diagram tools.*
- *Only those users who have a legitimate use for the Blue Prism software will be given access it*

System Control

<In this section System Control within Blue Prism should be outlined. This should include who will have the System Manager role, the level of Blue Prism knowledge required by that user, contingency to ensure a System Manager is always available (holidays, illness etc.)>

The authority to change the Blue Prism installation lies solely with the System Manager. This can only be carried out by a user with System Administration access.

- *Creating a new user or modifying the access rights of an existing user. A Blue Prism Account Request form must be completed and sign off obtained from the System Manager.*
- *The registering of new web services and other external services (such as Windows COM objects).*
- *Any database management changes, such as the configuration of the database archiver or changes to the product licence key*

Example user roles implementation

The following matrix depicts Blue Prism roles and responsibilities:

Permission Set	Role			
	BP System Administrator	BP Process Controller	VM Administrator	BP Release Manager
VMWare				
Log in (2 factor)		X		
Log Out	X	X	X	
Start Up	X	X	X	
Shut Down	X	X	X	
Restart	X	X	X	
View		X		
Interact		X		
Blue Prism (AD)				
Log In (AD)	X	X		X
Edit Schedule		X		
Edit Credential	X			
Import Release				X
Edit Process				
Start / Stop Process		X		
Blue Prism UAT				
Export Release	X			

Release Implementation

BP System Administrator	BP Process Controller	VM Administrator	BP Release Manager
	Stop processes		
Export Release			Import Release
	Edit Schedule		
Edit Credentials			
	Log into VMs		
	Start processes		

VM Restart

BP System Administrator	BP Process Controller	VM Administrator	BP Release Manager
	Restart VM		
	Log into VMs		
	Start processes		

Notes:

- In the above example the BP Process Controller, through Active Directory, is the only user with permissions in Blue Prism to start and stop processes (manually or via the scheduler). The VM Administrator is the only user with permission to log into a VM. The VMs can remain logged in, as the VM Administrator is the only user with permission to remotely connect.
- There is a full audit trail in place on both the VM connections and within Blue Prism to demonstrate exactly who has configured the scheduler to start these processes.
- The Process Controller cannot edit processes or import releases – this is the role of the Release Manager, who in turn cannot start or stop the processes or edit them in the production environment. Furthermore, the release manager cannot create or export a release from other environments.
- VM administrators only have access to restart, log off or shut down VMs. No-one has VM interaction except the BP process controller, who is responsible for the processes.

3.3. Blue Prism User Accounts

New Blue Prism user requests

<this section must outline how Blue Prism users are created or modified. What forms should be filled in? Who creates the user or adds the user to the domain group?>

Blue Prism Recommendations

- *A Blue Prism Account Request form must be completed and signed off obtained from the System Manager for every change to the Blue Prism user base. This includes new users, amendments to existing users and removal of users ahead of their system expiry date.*
- *By default a new user's account will be set to expire in six months' time with a password expiry every four weeks.*

Use of Blue Prism Single Sign-on

Blue Prism recommends the utilisation of the Single Sign on (Active Directory) feature within the product.

- *By enabling single sign-on, users of Microsoft Windows who belong to a corporate domain will automatically be authenticated to use Blue Prism on the basis of their user credentials and group memberships, whilst non-authorised users will remain locked out.*
- *By setting up Blue Prism to adopt corporate security policies to control access and user permissions within the software, large numbers of users can be granted access to the platform without requiring duplicate maintenance, and security policies can be readily implemented and effected using standard procedures.*

- *This places Blue Prism access control in the hands of the network administrator and provides a familiar and trusted mechanism for restricting access to important software.*
- *To distinguish between the permissions that each Blue Prism role is given within different environments (i.e. development, test, and live) different roles should be set up for each environment on the domain server (i.e. prod_bpcontroller, uat_bpcontroller).*

Blue Prism native logon

If the Blue Prism native logon features are to be utilised instead of the recommended single sign on, Blue Prism recommends that the password rules are set up to at least match the rules implemented by other systems in use in the organisation. For example:

- *Must contain a mixture of character types (i.e. upper-case, digits etc.)*
- *Must have a minimum length (i.e. 8 characters)*
- *Not show user names on the login screen or default the log in name*
- *Lock the user out of Blue Prism after a number of failed attempts (i.e. 3 attempts)*
- *Set user passwords to expire within a reasonable timeframe (i.e. 4 weeks).*
- *A users new password cannot match the last n passwords used (i.e. the last 4 passwords). Note: this option is available from Blue Prism version 4.2 onwards.*

3.4. System Accounts

This section of the security policy document relates to ensuring that the systems that Blue Prism uses in its automated solutions are used in a secure and appropriate manner in keeping with existing company policies.

Blue Prism accesses target systems much as a human user would and as such requires its own user names and passwords.

<Describe how system accounts are created, e.g. 'Target system accounts to be used by Blue Prism are to be obtained in the normal way following the client's standard procedures'.>

3.5. Credentials

The Credentials feature of Blue Prism provides a secure repository for log in details, storing them using Either AES or TripleDES encryption. AES-256 AesCrypto Service (256 bit) is recommended as the current highest level of encryption and is FIPS compliant. Credentials are responsible for determining which processes, resource PCs and users are able to access log in details, and for providing them on request if allowed by a set of permissions.

- *The System Administrator, acting with the permission of the System Manager, is responsible for storing system account details as Blue Prism credentials.*

<A section should appear here to describe each Blue Prism credential. Create a generic section for multiple versions of the same credential, e.g. Customer System 1, Customer System 2, 3, 4, 5 etc.>

System Name	<The name of the target system, e.g. 'Customer System'. Live and Test versions of an application should be treated as different systems.>
Credential Name	<The name of the credential, normally the same name as the target system. Normally the same credential name is used for Live and Test versions.>

Password Expiry	<The password lifecycle, either determined by the target system or as agreed with the customer, e.g. 'every day', 'every 90 days', or 'never'.>
Password Change Method	<The agreed method of changing an expired password, e.g. 'Credential manually changed by the System Administrator every 30 days', or 'Credential automatically changed by Blue Prism process every days'.>
Password Reset Method	<The agreed method of obtaining a password reset, e.g. 'Telephone request to IT Support by the System Administrator followed by manual update of credential'.>
Processes	<List the processes permitted to use this credential, e.g. 'Process A, Process B and Process C'.>
Resources	<List the resources (including debug resources) permitted to use this credential, e.g. 'XP0001, XP0002 and XP0002_debug'.>
Roles	<List the user roles permitted to use this credential, e.g. 'Developer', 'System Administrator' and 'Process Controller'.>

<Describe the option used for the location of the Credentials key(s)>

Blue Prism controls access to Credentials by means of a shared key, which will be stored in (delete as appropriate: a configuration file on the Blue Prism Server machine under C:\Documents and Settings\All Users\Application Data; the Blue Prism database; a configuration file on each machine under C:\Documents and Settings\All Users\Application Data).>

Blue Prism Recommendations

- *Credentials should be set up with the key stored on the BP Server machine, separate to the encrypted information on the database.*
- *System user accounts are usually allocated to Blue Prism in one of two ways, a separate account per PC, or a separate account per automated process. To minimise the number of system accounts that need to be created and maintained Blue Prism recommends that, if possible, a system account is created per process. Some systems allow a user to only log on once at any time, in such cases a user account will have to be created for each PC.*
- *(Note: If required, it is also possible for Blue Prism to retrieve credentials based on who is logged into the PC. This method may be used to ensure that the user logging into systems is tied to the user logged into the LAN).*
- *For maximum security it is possible for Blue Prism to change and store credentials in a way that ensures that no users within the organisation know what the passwords it uses are currently set to. This is done by creating a Password Change process for each system. If it is possible for a user to instigate a password change within the system we recommend that a Password Change process is scheduled to be run at regular intervals to change the password (i.e. daily or weekly). If it is not possible to instigate a password change, the process will need to be reactive and change the password only when the previous one expires.*
- *Blue Prism recommends that the credential key is securely backed up to ensure that encrypted data is not lost if the key is misplaced or overwritten.*
- *Data Gateways require a credential to be created as part of the installation.*
- *Out of the box integrations to Enterprise Password Vaults, such as CyberArk are possible in Blue Prism. These act as an exterior credential store.*

4. Environment Security

This section of the security policy document relates to ensuring that the environment in which the Blue Prism solution and the systems it accesses runs in is secure.

4.1. Database Access

<Describe the database access > method for each environment. If users are allowed access, what are the procedures for granting access and what privileges are afforded>

Blue Prism Recommendations

Blue Prism recommends that there is no direct access (i.e. not via the Blue Prism application) to the live or UAT databases permitted to Blue Prism users. The database user used by Blue Prism should only have read/write access to the Blue Prism tables. If increased permissions are required (i.e. to initially create the Blue Prism database, or to upgrade the database as part of a Blue Prism version upgrade), the relevant permissions should be given temporarily only until the creation/upgrade task is complete, and access should be monitored until the task is complete.

Blue Prism recommends the use of a BP Server architecture which marshals all access to the database from Blue Prism clients in a controlled and secure manner. For the use of a BP Server service, either SQL Authentication or Windows Authentication may be used. If Windows Authentication is to be used, an application service account on the BP Server machine will need to be given sole access to the database. For additional security, it is recommended that access to the Blue Prism database is restricted to the allocated database analyst staff (DBA) and the BP Server machine (and possible a contingency machine if one exists), by restricting IP address access with the use of Microsoft SQL or Firewall settings.

Using SQL Native authentication is not advised for Production environments as is it generally regarded as less secure than using Windows Authentication.

Data Gateways require a separate SQL Login and User creating as part of the installation.

4.2. Blue Prism Resource PC Security

<Details of the Resource PC environment and its security should be outlined here>

Blue Prism Recommendations

Virtual Machines

Blue Prism recommends the use of virtual machines (VMs) as resource PC's, running in a secure server-based environment. As well as Private Cloud, Public Cloud is also a viable infrastructure option for a Blue Prism environment. Currently Blue Prism recommends Azure, AWS or Google Cloud. For more information please see the Blue Prism Virtualisation Guide, or the Azure \ AWS \ Google Cloud reference architecture guides.

LAN Access

Access to live resource PC's will be limited specific LAN accounts allocated to the VM Administrators. Blue Prism recommends that the VM Administrators are not members of the Blue Prism solution team (i.e. not Process Controllers or Process Modellers), but instead staff from the Information Systems team that is providing support for the environment.

Physical Access

If the Blue Prism solution requires Resource PC screen locks to be disabled (dependant on the application modelling methods required), access to the physical machine must also be secured. This must be with the use of a secure location for the machines. For VMs this may be done with the use of security features in remote access software (i.e. limiting remote access to specific IP addresses or LAN users).

For full use of the Blue Prism Scheduler, the preferred Blue Prism solution is to leave VMs turned on and logged in so that tasks may be scheduled to start at specified times by Blue Prism users. This is possible by securing, limiting, and auditing access to the Blue Prism application and the VMs.

The alternative solution is for the VM Administrator on duty on any given day to log into the VMs each day and the Blue Prism Process Controller to manually start automated processes in the Blue Prism Control Room for the period he/she is on duty, and stop processes and log out of VMs at the end of their shift.

4.3. Data Security

<A data security policy should be outlined here with the following aims:

- *Data will be protected from unauthorised use and disclosure.*
- *Data will be stored in accordance with all relevant security, confidentiality and privacy policies in addition to the external legal and regulatory responsibilities.*
- *Data within Blue Prism will only be made available to users and systems if necessary for the completion of their respective tasks and if prior authorisation is granted by the System Manager.*

A list should be kept here of specific policies e.g. account numbers not to be visible in work queues, any stage handling credit card details to be have logging switched off etc.>

Blue Prism Recommendations

Client Data

- *Care should be taken during design and development to ensure that data protection policies (i.e. PCI, FIPSm HIPAA compliance) are kept to by the Blue Prism solution.*
- *Blue Prism logging will only be turned on to the minimum levels required to support the process and trace case routes and outcomes. For example, case ID's or customer ID's may be logged, but personal client information should never be logged.*
- *If client information is required to work an automated process, if possible, the information should only be stored in memory at runtime as transient data. If the information needs to be stored to the Blue Prism database (i.e. in a Blue Prism Work Queue item), it should be encrypted. Such information should be outlined in the Blue Prism solution design.*
- *The Blue Prism Work Queues may contain information to enable the automated solution to find a client in a host system and carry out the required actions. If this includes storing any sensitive information, it can only be stored encrypted.*
- *Any solution that involves the use of credit cards must be PCI compliant. PCI compliance must be incorporated into the solution design.*

Data retention

- *Blue Prism application audit information (user activities within the product) are not deleted by default and will remain in the Blue Prism database until they are removed by housekeeping scripts. It is recommended to run housekeeping scripts are regular intervals.*
- *Session log information should be kept for a time period in adherence to standard organisational data retention policies. This may be in an archived format that can be retrieved if required. (I.e. logs should be retained 2 years).*
- *Session log information can be archived or deleted from the Blue Prism database. The minimum amount of operational data should be kept in the Blue Prism database. If more is required to adhere to standard organisational data retention policies then these should be archived into another data source using the in-built archiving facility in the GUI, Data Gateways or a custom solution to a Data Warehouse or MI application. It is recommended to only keep 30 days with the Blue Prism Database itself.*
- *If Blue Prism session logs need to be exported and sent to Blue Prism consultants to assist in support, the logs should first be evaluated to ensure that they contain no client or organisationally sensitive information. Log files should be compressed, and password protected before being sent.*
- *Organisation information relevant the Blue Prism solution can only be shared with Blue Prism staff if an appropriate non-disclosure agreement has been put in place.*

Note:

- It should be noted that the Blue Prism password datatype only obscures information to user and therefore should only be used at runtime. Blue Prism credentials should be used for storing sensitive information.

5. Periodic Security Reviews

<Details of who will carry out security reviews, how often they will occur, and what they will involve should be outlined here>.

Blue Prism Recommendations

There should be regular reviews of the Blue Prism solution with the following aims:

- *Ensure the policies outlined in this security policy document are fully adhered to*
- *To look for any new security weaknesses that may have been created in the solution and update the security document accordingly*
- *To audit the use of the Blue Prism application and the Blue Prism Resource PCs to ensure they are not misused.*
- *Ensure data protection policies are adhered to*

Reviews should be done by staff not involved in the day to day running of the Blue Prism solution (i.e. IS Security staff

6. Blue Prism Solution Design Documents (SDDs)

Detail here who should sign off SDDs on behalf of security, and who the designer should contact with and security concerns or questions>

Blue Prism Recommendations

Design Authority

- *The author of Solution Design Documents should take care to ensure that any policies outlined in the Security Policy are met by the design. Any aspects of the design that may impact on security, but are not answered by this document should be referred to nominated security staff and this policy document should be updated if required.*

Security Sign Off

- *A person or team should be identified with the responsibility to sign off all Blue Prism solution design documents as passing the security policy. Blue Prism processes should not be migrated from the development environment until this sign off has been received.*