Title:	**Policy NCDHHS Robotic Process Automation**
Revision History:	**Jan 2022, Jan 2023, Jan 2024, Jan 2025**
Original Effective Date:	**March 2021**

SCOPE:

NC DHHS Divisions and Offices

PURPOSE:

To establish security requirements for NC DHHS use of Robotic Process Automation (RPA).

POLICY:

DHHS Divisions and Offices shall implement policies and processes to defend against the security risks of using Robotic Process Automation (RPA) for accessing DHHS information resources. The following baseline security policy provisions shall apply to DHHS Divisions and Offices personnel who are responsible for the installation, operation and security of RPA technology.

The following RPA roles are defined for this policy: All individuals who utilize the State of NCDHHS information technology (IT) resources are responsible for adhering to this policy.

RPA Roles	Scope and Responsibility
Program Manager	RPA Program Business Unit level business user role responsible for implementing the RPA software or managing the RPA service in compliance with federal, state security policies. For a centralized program this is a single central role. For a decentralized program there can be more than one program managers.
Business Process Owner	Robot Business unit role that is responsible for the RPA robot lifecycle. This role has responsibility to draft the use case, process design document, interacting with RPA solution architect, RPA Developers, RPA Server Administrators and System owners, and interacting with security official for reviews and approvals.
Robot Solution Architect	Robot Business unit role that is responsible for architecture and design in support of the use case defined by Business Process owner.
Robot Process Developers	Robot Business unit role with responsibility to develop and train of the Robots
System Owner	DHHS or external business user who approves the use of RPA robots to access their applications/systems for a specific set of actions
Information Security Official (ISO)	This is a division specific role responsible for security policy compliance. This role provides inputs at architecture, design, operation/access level.

The following baseline security policy requirements apply to the above RPA roles:

1. **Program Manager** shall ensure that RPA platform or managed service complies with the below requirements. Specifically, Program Manager shall ensure that:
    a. RPA Platform is Secure:
        i. System integrity is maintained:
            A. only authorized administrative users can install and/or update the RPA software if RPA platform is hosted at DHHS, or manage the RPA service if it is hosted externally,
            B. RPA software version is up to date and patched by DHHS or the entity that DHHS designates for hosting the RPA software,
            C. changes to RPA platform that may impact security are reviewed by DHHS level
            (CISO) security office,
        ii. There is strong accountability for all RPA platform level activities:
            A. logins and other access to the RPA Server software (used for managing the robot workflows and credentials) shall be authenticated using enterprise credentials (NCID/EADS) and Multi-factor Authentication,
            B. all logins and other accesses to the RPA Server are logged,
            C. RPA platform and Robot logs cannot be deleted or tampered with,
            D. logs are aggregated and are monitored manually as per federal and state security log monitoring requirements,
            E. there is a secure backup of the RPA platform logs and Robot logs and the backup copy is maintained as per federal and state policies for log retention,
        iii. There is strong monitoring of all RPA platform activities:
            A. administrative user access is monitored periodically and revoked after completion of their duties in compliance with federal and state administrative access revocation requirements,
            B. incident management is notified of any suspicious activity in logs,
    b. Business units that use RPA Robots enforce Security for Robots:
        i. Secure development, testing and change management processes are followed for Robot development and training,
        ii. Each Robot within the RPA platform shall use an identity that shall:
            A. be non-human identities that conform to enterprise's non-human identity and credential policies,
            B. be unique specific to a single use case (workflow) supported by that Robot. The Robot identity will follow a naming convention that allows identification of the Robot owner and use case,
            C. not include information that identifies it as a Robot (e.g., BOT, ROBOT, RPA, and RPA product names are not allowed in the Robot login names),
            D. only be authorized for the functionality that has been documented, tested, reviewed and approved for that Robot,
            E. not used for other functions such as admin access to Robot VMs, or user access to applications

iii. Robot passwords shall comply with federal and state password policy requirements,
    A. Robot passwords are kept updated on a timely basis in a secure manner (passwords shall not be shared)
iv. Robot credentials (identity and secret) shall be stored with encryption
    A. with FIPS 140-2 (Level 2 or higher preferred) compliant encrypted storage and accessed only by authorized administrators,
    B. keys used to protect the credentials are held and managed by DHHS administrators in compliance with federal and state key management requirements,
v. All logins and accesses by Robots will only use encrypted connections and encrypted data at rest in compliance with federal and state policies,
vi. There is a secure backup of each version of the Robot and maintain the backup copy after Robot has been retired and is retained as per the federal and state policies.

2. **Business Process Owner** shall ensure that each new or updated Robot complies with the requirements below. Specifically, Business Process Owner shall ensure that:
    a. Robots have a well-defined, documented, acceptable and predictable behavior (AI based dynamic behavior is strictly not allowed). Robot shall not be used for:
        i. security related functions such as log monitoring, password resets,
        ii. mass dissemination of sensitive information (PII or PHI),
        iii. data deletion,
        iv. privilege escalation,
        v. denial of service,
    b. Robot development follows strict lifecycle, change management and acceptable use requirements:
        i. in addition to complying with state policies for change management for each Robot, strict change management is enforced between each Robot and the set of applications that the Robot interacts with,
        ii. ensure that application changes that may impact Robot functionality shall be documented and tested to ensure that no new risks are introduced,
        iii. number of Robots that concurrently perform login and Number of Robot based concurrent access to each application are established at the start of the Robot approval process based on discussions with authentication service providers and application system owners,
        iv. Robot behavior is rigorously tested so it only performs the functions that are fully documented and no other functions, and there is no risk to confidentiality, integrity or availability of data,
    c. The following authorization and separation of duties are enforced:
        i. business level written approval has been obtained from System Owners of DHHS or external applications to allow Robots to access their applications
        ii. training of a Robot shall be restricted to authorized users who have expertise in RPA technology including designing and updating the Robot's workflows, securely storing and refreshing the credentials

iii. Robot developers/trainers are not allowed to run Robots in Production and are not able to access any Production applications or data,
iv. Operational staff are not allowed to update the Robots (only developers/trainers are)
v. Production Robots will use identities and secrets that are different from Development Robots
vi. Production identities are only available to operational staff and not to developers,

d. there is strong accountability throughout Robot lifecycle:
   i. Robot workflow creation and updates are logged in tamperproof audit logs, and logs are monitored,
   ii. credential storage, access and updates are logged, and logs are monitored
   iii. Incident management is notified of any suspicious activity in logs

Procedure

The following baseline security procedures will be followed:

1. Program Manager
   a. for each new or enhanced RPA platform/technology, initiate a full security review by submitting an RPA Platform Security Questionnaire and supporting documentation to the DHHS security office
   b. for each new Robot, identify the business unit and the corresponding Robot Business Process Owner who will be responsible for the Robot lifecycle;
   c. new approval is obtained from the DHHS security office:
      i. for any changes to the RPA platform, architecture, design, access or security
      ii. once a year by providing updated documentation (listed above)
2. Business Process Owner
   a. for each Robot (RPA use case), the following roles are identified – Solution Architect, Robot
      Process Developers, RPA Server Administrators, Robot Administrator(s), System Owner(s)
   b. for each Robot, approval is obtained from the division ISO by submitting the RPA Robot Security Questionnaire for the RPA use case to your security official (division ISO)
   c. for each Robot, new approval is obtained from the division ISO:
      i. for any changes to the Robot use case, architecture, design, access or security
      ii. once a year by providing updated documentation (listed above)