CYBER GUIDELINE DOCUMENT

NCSP Robotic Process Automation

ABSTRACT:
This guideline describes best practice risk management controls for using Robotic Process Automation (RPA) for the purpose of automating manual administrative overheads for National Policing Forces and applications.

This document only provides guidelines to automating manual processes and is not intended for machine learning (ML) or artificial intelligence (AI) derived solutions. Please refer to separate guidelines and standards for Digital Process Automation (DPA), AI and ML related activities.

ISSUED	October 2024
PLANNED REVIEW DATE	October 2025
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

COPYRIGHT: Police Digital Service

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing guidelines in relation to Robotic Process Automation.

Introduction

Robotic Process Automation (RPA) is technology in the form of software applications designed to mimic human interactions with digital systems, such as searching, entering data, and extracting information from systems, documents, websites etc.

RPA aims to streamline and automate routine and manual processes that are typically performed by humans. In some instances, RPAs are commonly termed as 'Web Robots', 'Bots', 'software robots' or 'Digital Workers'. These terms can be used interchangeably by the national police forces, but they should all be read and utilised within the context of this guideline. Any national police force looking to implement any type of RPA, bots or web bots should consider this guideline for designing, developing and implementing the RPAs / bots in a secure and efficient manner which is fit for national policing forces and applications.

Automated processing of data requires careful consideration from a cyber threat perspective as such services are attractive to cyber threat actors. Automated services present opportunities for unsupervised access to systems or data, excessive loading, denial of service, process poisoning or interruption amongst others. The use of RPA supported by this guideline and Secure By Design principles, should be supported by robust risk assessment and management in the context of the criticality of process and data associated with it.

This guidance only refers to process automation including rules-based decision making, it does not cover the use of process automation to conduct automated decision-making, such as Artificial Intelligence (AI). Any automated decision-making needs careful consideration, as Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or

COPYRIGHT: Police Digital Service

similarly significant effects on them.[1] In these circumstances consultation with the Data Protection Officer is essential.

If the data being decided upon relates to nominals etc, then the Management of Policing Information (MoPI) rules around automation, human decision making and data quality confidence may also apply.[2]

In all cases a Data Protection Impact Assessment needs to be completed where process automation is accessing Personally Identifiable Information (PII).

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guidance is to ensure that process automations are implemented following best practices and using industry recognised frameworks and standards that are fit for purpose for National Policing and to enhance risk-based decisions required to implement RPA securely and effectively.

Audience

Force / organisational Senior Information Risk Owners (SIROs), Information Security Officers (ISOs), information security practitioners, Information Asset Owners (IAOs) and Dev teams.

Scope

This guidance should be referred to as part of any decision-making in relation to the selection, procurement, deployment and use of any technology related to Robotic Process Automation (RPA), Web-Bots or Bots within the National Policing.
Any other engagements related to Digital Process Automation, machine learning or artificial intelligence is beyond the scope of this guidance.

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/
[2] https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal

COPYRIGHT: Police Digital Service

Requirements

The tables on the following pages describe the best practices for governing, assessing, deploying and monitoring Robotic Process Automation solutions. It does not replace existing security assurance and risk management activities applied when bringing in any IT system in Policing.
They should not be considered an exhaustive list, however, can form the basis of a risk-based approach.
They have been produced based upon various sources including Forces that have been consulted, RPA solution leading providers and best practice guidance.

Aspect	Guidance
1.0 Process assessment and selection	• Implement a process to assess requests for Robotic Process Automation of local force business processes against criteria including complexity, benefits and data privacy impact. • Look for processes that are repetitive, rule-based, high in volume, and have a significant impact on productivity and accuracy. • Care should be taken to not link together multiple RPAs in a process as this could inadvertently lead to automated processing. • Automated rules-based decision-making which modifies or deletes Personally Identifiable Information (PII) needs careful consideration by Force Data Protection Officers.
2.0 Normalise and enhance processes	• Before automating a process, streamline and normalise it to eliminate unnecessary variations and complexities. • Note that automating a process will not necessarily make it efficient and effective. Processes that need re-engineering are not suited to automation.
3.0 Effective governance and collaboration	• Establish a governance framework to oversee Robotic Process Automation implementation. Ensure consultation with the Information Security Officer, Data Protection Officer and IT teams from the outset. • Business process owners need to own and manage their respective Automated processes. • Define roles and responsibilities clearly, and ensure collaboration between Information Asset Owners, business stakeholders, IT teams, and Digital Process Automation developers. • In line with local Data Protection Policies, a Data Protection Impact Assessment needs to be completed where an automated process is accessing Personally Identifiable Information (PII).

COPYRIGHT: Police Digital Service

Aspect	Guidance
	• It is recommended that local 'asset' registers of automated processes are established and maintained. • Regularly communicate and share updates to maintain alignment throughout the implementation. • Ensure that Business Continuity Plans reflect automated process deployments and that there are adequate disaster recovery plans in place.
4.0 Security and compliance	See the Common steps to securely implement Robotic Process Automation section for more details. • Pay close attention to security and compliance requirements when implementing process automation. This specifically includes conducting Data Privacy Impact Assessments (DPIAs) in consultation with the Data Protection Officer. • Ensure that any digital process automation platforms / infrastructure is subject to security assurance (such as Secured By Design) prior to any RPAs being operational with live or Personal Identifiable Information. • Consider the differing risks presented by on-premise, hybrid and Software As A Service (SaaS) approaches. • Implement necessary security measures to protect sensitive data and ensure compliance with relevant regulations and policies. • Each process automation agent shall be issued a unique user account ID with the least privileges necessary to perform its function. • All Robotic Process Automation accounts (often referred to as Digital Workers) shall be subject to Force / National system identity & access management (IAM) policies. • Whilst enforcing a single Digital Worker account per automated business process represents a lower security risk, it may be more cost effective to cluster similar processes against a single Digital Worker identity. This is subject to a risk assessment and local Governance agreement. • Digital Worker identities for National Systems shall be issued for a single purpose only in line with the policies for that system. • Local Digital Worker identities re-use is subject to local Identity Management policies and governance. • Digital Worker identities for National Systems shall not be re-used.

COPYRIGHT: Police Digital Service

Aspect	Guidance
	• Automated process activity shall be subject to Force / National system auditing policies. • Monitor and audit the automated process & Digital Worker Identities in line with vulnerability management policies to identify and address any potential security vulnerabilities. • If Robotic Process Automation identities are required to connect to national applications, it must adhere to the level of security posture required by the specific national application as deemed secure at the time of the request.
5.0 Scalability and flexibility	• Design the Robotic Process Automation solution with scalability in mind due to the local force application restrictions. • In terms of connecting to national applications, specific approval needs to be sought which should be considered case by case basis. Requests should detail expected loading including size and number of requests expected over an agreed period. • Consider future growth and the ability to handle increased process volumes. • Ensure the Robotic Process Automation implementation is flexible and adaptable to accommodate changes in the processes or underlying systems (within local forces). • Have a business fallback plan in case the process automation needs to be switched off / disabled. Consider implementing a Process Definition Document (PDD) to detail the steps taken to perform a process. Give consideration that over time users will have knowledge/skill fade of process or be new to dept and not know process. Therefore, if an automated process is down backlog could build up whilst staff endeavour to replicate robot worker.
6.0 Error handling	• Implement robust error handling and exception management mechanisms within the Robotic Process Automation bots. • Account for potential exceptions or variations in the process flow and define appropriate actions for error resolution or escalation. • Retain logs in accordance with Protective Monitoring Policies. • Regularly monitor error logs and refine the bots to minimize errors and interruptions.
7.0 Continuous monitoring and optimisation	• Regularly monitor the performance of Robotic Process Automation bots and measure key performance indicators (KPIs) to evaluate the effectiveness of automation.

COPYRIGHT: Police Digital Service

Aspect	Guidance
	• Controls should be in place to monitor and manage loading such as size and number of requests to prevent excessive service consumption or denial of service attacks. • Implement quality checking mechanisms commensurate with the risk associated with the process being automated. • Analyse the data to identify areas for improvement and optimisation. • Implement enhancements and updates to continuously optimise the Robotic Process Automation solution.
8.0 Effective change management	• It is key to keep the personnel involved in the RPA development process understand the purpose of Robotic Process Automation, its benefits, and how it will impact their roles. • Implement effective change management strategies to address any resistance to change and ensure smooth adoption of automation. • Maintain appropriate records and change governance as the service is optimised/adapted over time.
9.0 Collaboration with IT/SECOPS	• Collaborate closely with IT and Information Security throughout the Robotic Process Automation implementation process. • Involve IT in the selection of the Robotic Process Automation tool, infrastructure setup, security considerations, and integration with existing systems.
10.0 Continuous learning and improvement	• Adopt a culture of continuous learning and innovation around Robotic Process Automation. • Encourage colleagues to share their insights, ideas, and suggestions for process improvement and automation. • Stay updated with the latest Robotic Process Automation trends and advancements to leverage new technologies and approaches.

COPYRIGHT: Police Digital Service

Common steps to securely implement Robotic Process Automation :

Aspect	Guidance
11.0 Data protection	• Implement strong data protection measures throughout the RPA lifecycle. • This includes encrypting sensitive data, securely storing credentials and access keys, and implementing secure data transfer protocols.
12.0 Access controls	• Implement strict access controls for Robotic Process Automation tools, bots, and associated systems. • Follow the principle of least privilege, granting access only to authorised individuals who require it for their specific roles. • Regularly review and update access permissions to ensure they align with business requirements. • When national applications are in scope, ensure NIAM or national application access control requirements are followed.
13.0 Secure development practices	• Apply secure coding practices when developing Robotic Process Automation bots or scripts. • Avoid hardcoding sensitive information in code, such as passwords or API keys. • Use secure programming techniques, input validation, and proper error handling to minimise the risk of vulnerabilities. • Ensure adequate testing of RPA environments and automated processes prior to deploying a production environment.
14.0 Authentication and authorization	• Implement strong authentication mechanisms for users and bots accessing the Robotic Process Automation systems. • Use multi-factor authentication (MFA) for user accounts and ensure that bots authenticate securely to interact with target systems. • Where MFA cannot be enforced, suitable security measures shall be agreed with the Information Security Team. • Additionally, implement role-based access control (RBAC) to enforce appropriate authorisation levels.
15.0 Secure configuration management	• Maintain a secure configuration for Robotic Process Automation tools and systems. • Regularly update and patch the software and underlying infrastructure to address known security vulnerabilities. • Configure firewalls, intrusion detection systems (IDS), and other security controls to protect Robotic Process Automation components from unauthorized access.

COPYRIGHT: Police Digital Service

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this guideline can also form part of regular cyber management reporting.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

COPYRIGHT: Police Digital Service

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial Version	13/06/2023
0.2	PDS Cyber	Initial internal peer review and updates following RPA working group feedback	27/06/2023
0.3	PDS Cyber	Updated further to NCPSWG review	05/07/2023
1.1	PDS Cyber	Aligned to new template, updates following feedback	08/2024

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	05/07/2023
1.1	NCPSWG	National Cyber Policy & Standards Working Group	02/10/2024

COPYRIGHT: Police Digital Service

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

COPYRIGHT: Police Digital Service