# RPA FAQ’s

### Are RPA Bots Safe?

In short “yes” provided that care is taken to ensure the bot has no more access than is required to undertake the task at hand, and only has access to the systems it needs to access to achieve them. This is the same principle that should be applied when providing staff with access privileges to systems. This is called the Principle of least privilege.

### Should bots have their own class of password? Or can we allow a bot to use a staff member’s credentials to login?

Under no circumstances should a bot be provided with employee credentials for ANU systems. This is because ANU staff credentials support Single Sign On. This means a single password would provide access to more than one system, and would not comply with the principle of least privilege.

The outcome of the above is that bots should be issued with its own password, which has access privileges sufficient only to achieve the task.

### What about programmers potentially hiding malicious code or back door code into larger systems?

RPA tools support code to written in a manner that supports discrete module functionality. This means that modules can be written to achieve simple reusable activities. For example a login routine for ARIES would be discrete, and reusable only for that function. This keeps the code simple and direct. The University of Melbourne have instigated a practice of every module written, should be reviewed by 2 other programmers. The simplicity of each module reduces the review overhead of the module and mitigates the risk of malicious code. In addition reusable modules reduces both development and review effort.

### How should bots be tested?

In addition to bots being tested in Test and Acceptance environments, supervised tests should continue in Production until the system owner is satisfied that the release is robust.

### How do we guarantee the security of RPA extracted data?

The University of Melbourne have instigated a practice that any data extracted into CSV or excel-like files are uploaded in to a secure database and subject to the same access privileges as the system it was extracted from, the CSV files are then destroyed. The ANU may employ similar processes in future.

### How should RPA skills be distributed across an organisation?

The University of Melbourne (UniMelb) has adopted a central team approach providing RPA skills and solutions across the university. The reasons behind this include the ability to support the practice of developing in modules and having access to resources to undertake code reviews. UniMelb were reluctant to allow distributed development of RPA solutions due to solutions being more likely to be siloed, unscaleable, poorly supported and vulnerable to changes in any centralised systems. A centralised approach guarantees a consistent development approach, and practice. The approach UniMelb have taken, and the risks of distributed RPA solution development is supported by the research. The ANU may follow a similar implementation model.

### Is RPA just a stop-gap solution?

RPA can be used as a stop-gap solution, but this doesn’t meant that it is always a stop gap solution. RPA can be used as a mechanism to share data between systems in cases where it is sorely required, while a more robust or comprehensive solutions are simultaneously being developed. This is a completely appropriate use of RPA considering the light and nimble nature of the tool and its rapid development time.

On the other hand, and on the more complex end of the spectrum, RPA can also assist a staff operator undertake complex on-boarding task that involve several systems in a manner that would make sense to improve a business as usual process in a robust manner and be designed as a long term solution.

### What is the difference between “unattended” and “attended” bots?

Unattended bots usually describe simple processing bots that do not require intervention. The function is similar to typical batch processing. The bot is triggered, and a result is delivered. An attended bot is one where the bot operates with the assistance of a staff member.

The need for an attended bot could be due to

* The complexity of the task at hand
* The opportunity for the bot to prepopulate a next step
* The need for a staff member to add value to the data or the process, or
* governance to ensure that policy obligations have been met.

### How could you phase the development of RPA skills in an organisation?

RPA can be divided into 3 basic types of implementation.

Type 1 (unattended): automation of copy and paste like functions where data is copied from one system to another, or copied from a system to create a report. In effect, a bot undertaken to do this kind of work replicates activity that is already undertaken by staff as a substitute to an API. It is important to note that the staff member does not add value to the data in this activity.

Type 2 (unattended): As with type one but the staff member may make simple non-discretionary decisions about the data. If the data item is more than this, it goes into this column, if value is zero, this happens etc.

Type 3 (attended): Where a bot can instigate or direct process based on data.

**Marketo**

Examples of this are University of Wollongong vertical 3rd party cloud application “marketing automation” ~ Marketo. Similar examples could be process such as student registrations process, payment process etc.

**Centerlink Robo Debt**

Another example in this category that has recently been in the news is Centrelinks Robo debt system for pursing overpayments and identifying fraud in government support payments. In effect his system is run as an unattended process and the outfall of this approach has been one where it is difficult to identify where governance and responsibility falls into question.

In effect this system looks for discrepancies in claims and income, sends a request for evidence, if no response is received or no satisfactory explanation is provided

### Summary of RPA practice

* Bots will be used with specific bot passwords that have been created with access privileges based on the “principle of least privilege”.
* RPA routines will consider “privacy by design” to ensure protection of data. This includes protection of data at the level of which data is extracted, or reports generated.
* Bots will be developed as reusable modules to encourage simplicity of code, and to facilitate code reviews.
* Code developed by a programmer will be independently reviewed by other two programmers to establish maintainability, security exposure, and functionality prior to release.
* RPA should be developed centrally to ensure scalability, maintainability and that governance protections are maintained.
* Each RPA project undertaken will consider privacy, complexity and risk exposure prior to commencement of the project.