

Be a guardian of your galaxy by implementing your Identity Governance strategy, it's that simple!



Pim Jacobs 
Principal Consultant
InSpark



Jan Bakker 
Microsoft 365 consultant
Jan Bakker consulting



Jan Bakker

Freelance Microsoft 365 consultant & Microsoft MVP

- Microsoft 365 | Security | Identity & Access
- Blog: janbakker.tech
- Twitter: [janbakker_](https://twitter.com/janbakker_)
- LinkedIn: <https://www.linkedin.com/in/jan-bakker/>





Pim Jacobs

Principal Consultant @ InSpark & Microsoft MVP

- Focus on the full Entra portfolio
- Blog: identity-man.eu
- Twitter: [@pimjacobs89](https://twitter.com/pimjacobs89)
- LinkedIn: <https://www.linkedin.com/in/pimjacobs89/>
- Soccer | F1 | Family time





Agenda

- Introduction of Identity Governance
- Joiner process
- Mover process
- Leaver process
- Considerations & next steps
- Questions





SECURITY

Introduction of Identity Governance





Introduction of Identity Governance

01

Identity Lifecycle & Workflow Management

Joiner Mover Leaver process

04

Azure AD PIM

Just in time just enough access

02

Controlling 3rd party apps

Access and provisioning to 3rd party apps

05

Requiring a 'Terms of use'

For employees and guests

03

Access Lifecycle Management

Access Packages and Reviews

06

Reporting

Improve current setup





SECURITY

Introduction of Identity Governance

01

Identity Lifecycle & Workflow Management

Joiner Mover Leaver process

03

Access Lifecycle Management

Access Packages and Reviews

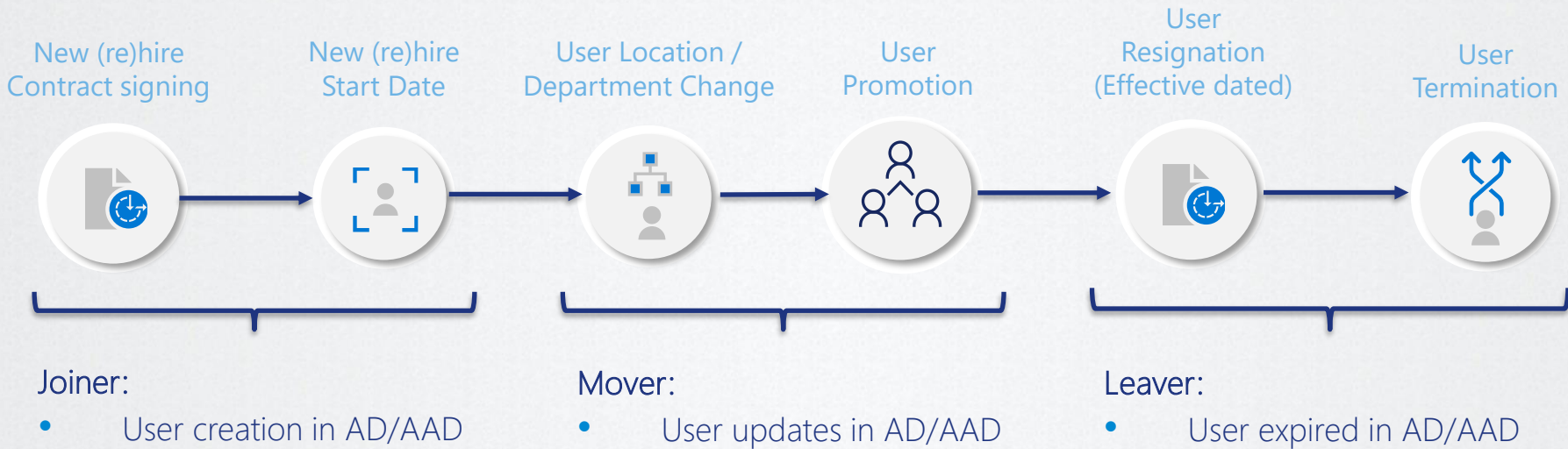






SECURITY

Account Lifecycle Management



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft

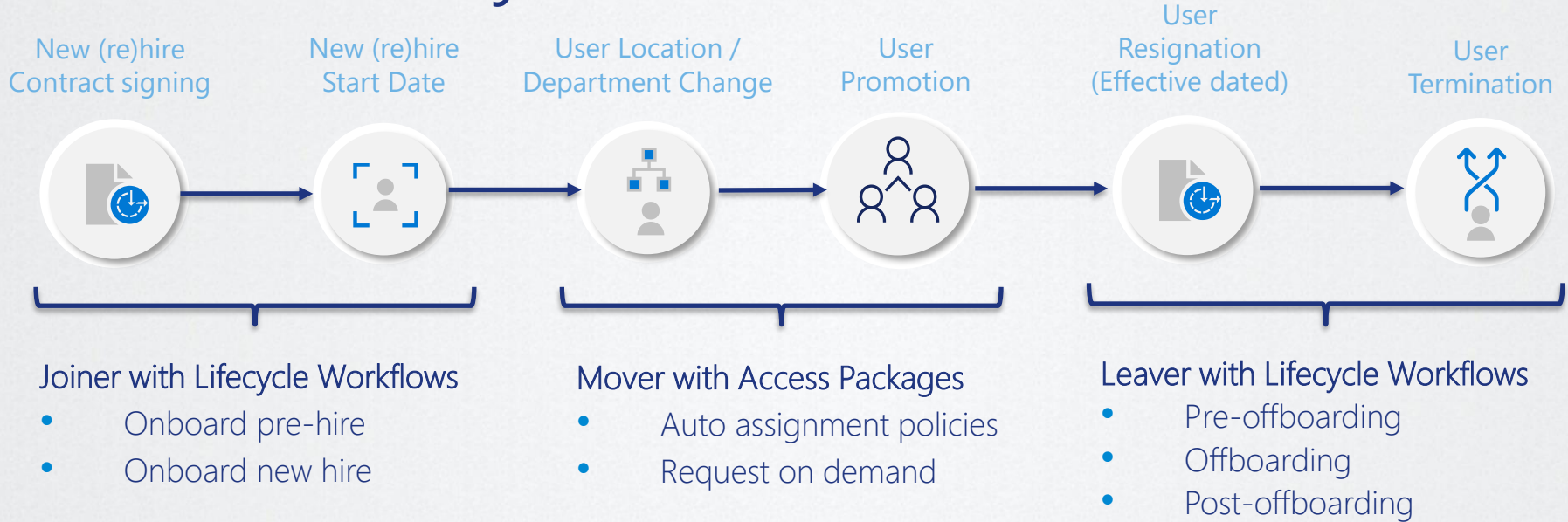
Account Lifecycle Management

Lifecycle management explained

- Lifecycle management is important for **all end user accounts**.
 - Accounts are therefore **provisioned** and **expired/disabled** on time in AD /AAD.
 - HR data becomes the **source of truth**!
 - **HR is responsible** for the data.
 - Today only supported with **SAP SuccessFactors & Workday**
-
- **NOTE:** Make sure you've implemented lifecycle management around **guest accounts** as well **by using Access Reviews**.



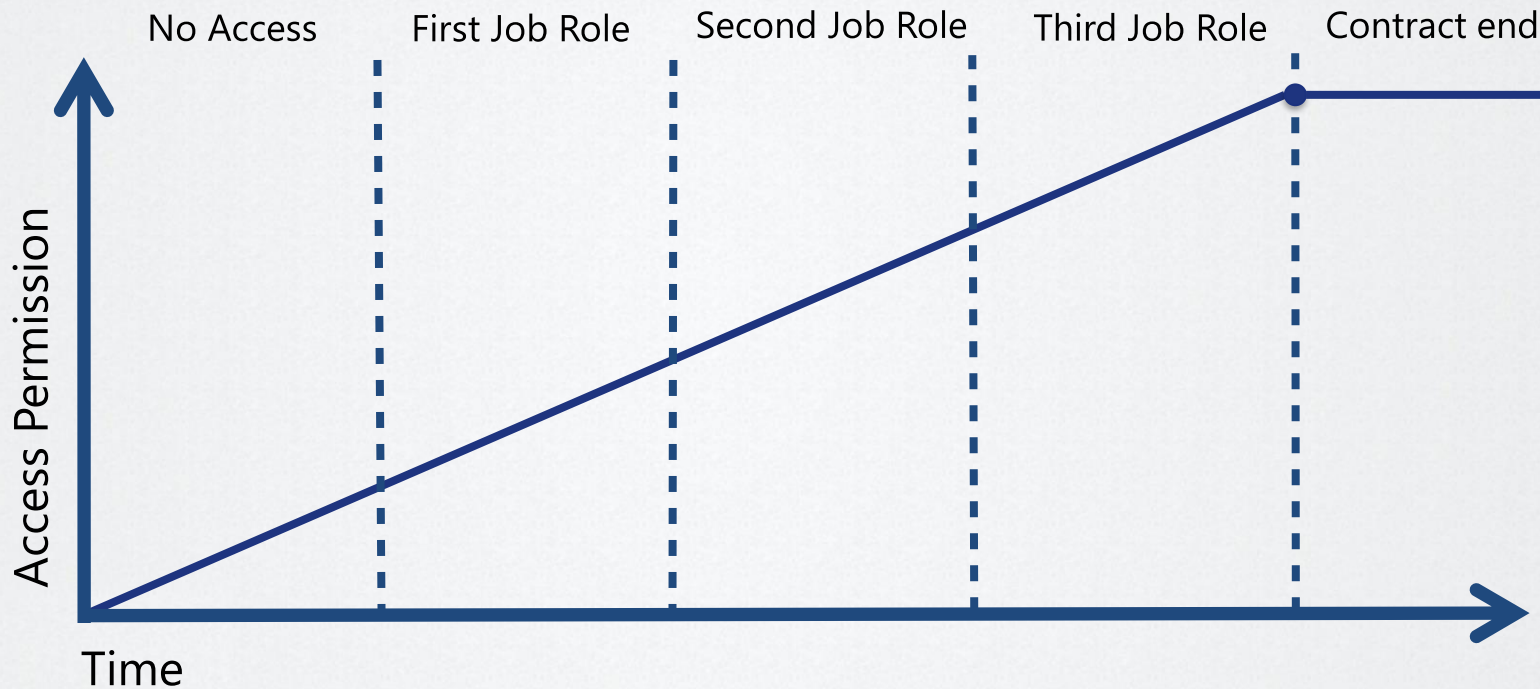
Lifecycle Workflows





SECURITY

Lifecycle Workflows



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

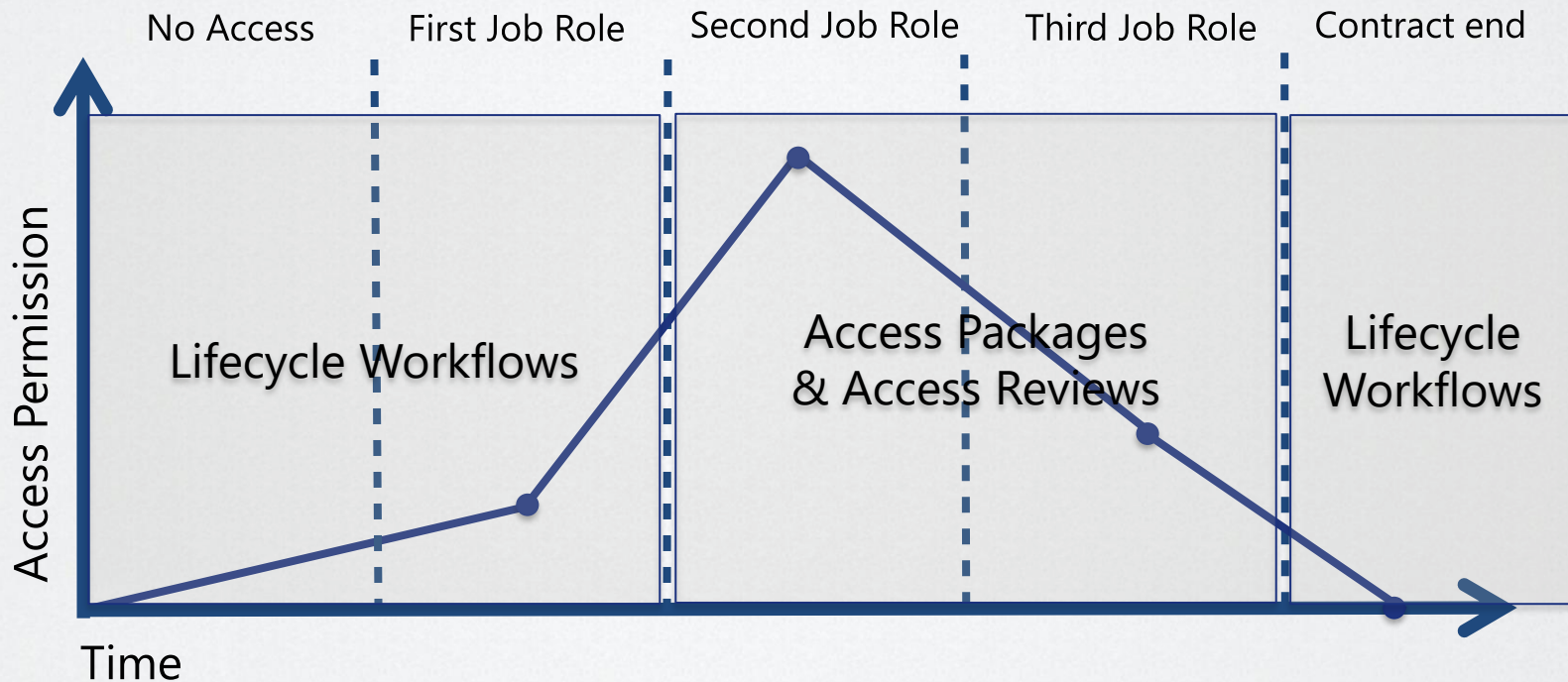
INSPARK

Microsoft



SECURITY

Lifecycle Workflows



InSpark

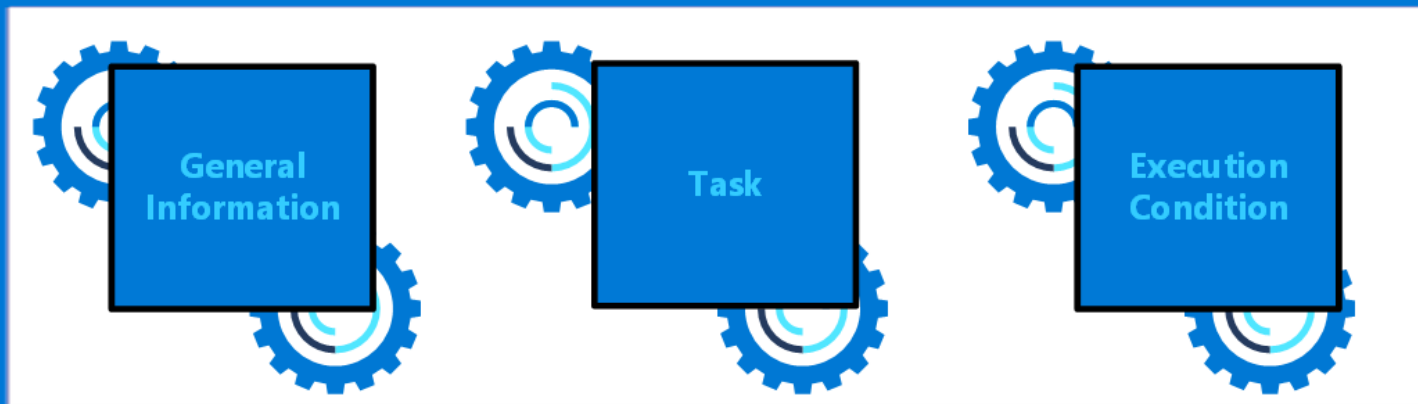




SECURITY

Understanding Lifecycle Workflows

Lifecycle workflows

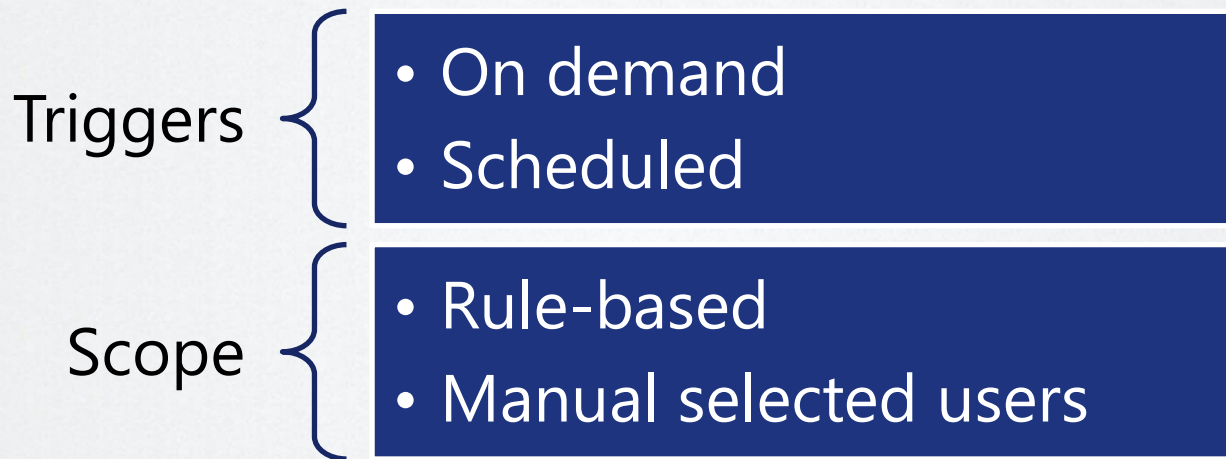


Automate JML





Execution conditions



Lifecycle Workflows facts



Runs each 3 hours



Interval is customizable (1-24)



Max 50 Workflows per tenant



25 per tasks per workflow



PreferredLanguage

PATCH <https://graph.microsoft.com/beta/identityGovernance/lifecycleWorkflows/settings>
Content-type: application/json

```
{
  "workflowScheduleIntervalInHours": 8
}
```



Native Azure AD by default



EmployeeHireDate



EmployeeLeaveDateTime



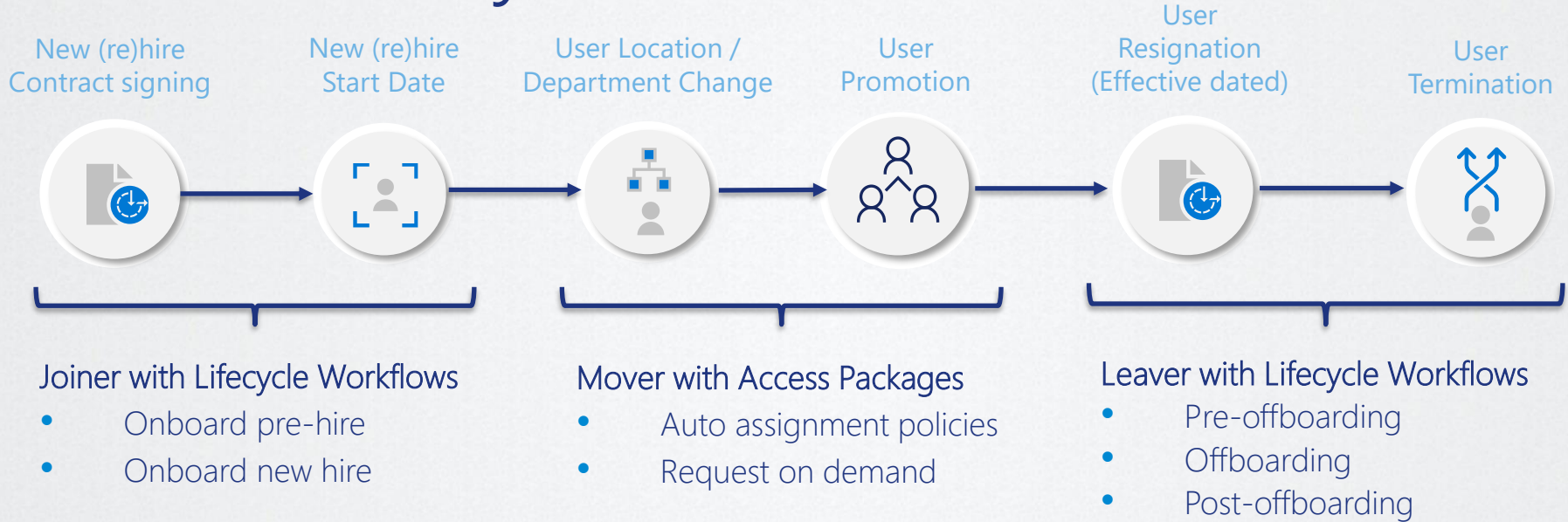


SECURITY

Joiner with Lifecycle Workflows



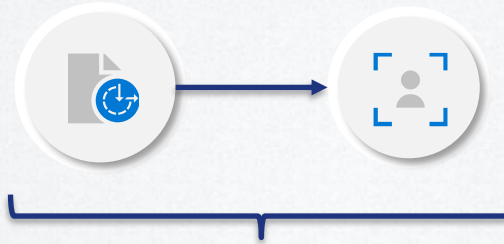
Lifecycle Workflows



Lifecycle Workflows

New (re)hire
Contract signing

New (re)hire
Start Date









Joiner with Lifecycle Workflows

- Onboard pre-hire
- Onboard new hire



Onboarding Tasks

-  Add user to group
-  Remove user from group
-  Enable or disable User Account
-  Generate TAP and send to manager
-  Send welcome mail
-  Add to selected Teams
-  Run custom task extension





Example

- **Task:** send welcome email
- **When (trigger):** Seven days before the NewEmployeeHireDate attribute value
- **Who (scope):** new employees in the Marketing department





SECURITY

Lifecycle Workflows

Available workflow templates for joiners:

 Joiner

Onboard pre-hire employee

Configure pre-hire tasks for onboarding employees before their first day

[Select](#) | [Details](#)

 Joiner

Onboard new hire employee

Configure new hire tasks for onboarding employees on their first day

[Select](#) | [Details](#)



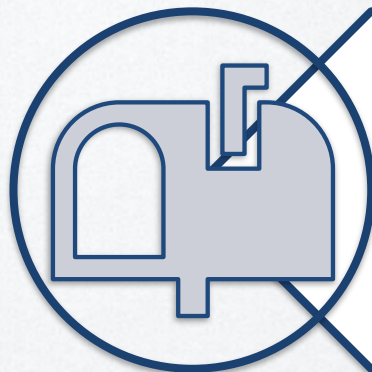


SECURITY

Tasks



Generate TAP
and send to
manager



Send
welcome mail



Welcome to your new team, Allan Deyoung



Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>

To: Allan Deyoung



Thu 9/22/2022 12:40 PM



Welcome to the team, Allan

We're excited to have you join our growing team and look forward to a successful and memorable journey together.

We've already set up a few things to help you get started quickly and make your onboarding process as smooth as possible.

For more information and next steps, please contact your manager, [Nestor Wilke](#)

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Reply

Forward



Allan Deyoung, your new team member will be joining soon



Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>

To: Allan Deyoung



Thu 9/22/2022 12:50 PM



Rachel will be joining the team soon

Your new team member, **Rachel Green**, is scheduled to join the team on **Friday, 30 September, 2022 22:00:00 UTC**.

To help make the onboarding process as smooth as possible, we've generated a temporary access pass for Rachel to use as their temporary password when signing in for the first time.

The temporary access pass is **27KXduac**. Please share it with Rachel so that they can sign in on their first day and start setting up their secure credentials. Your admin has configured this pass to expire on **Friday, 07 October, 2022 22:00:00 UTC**.

If you have questions, please contact HR or your admin.

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Reply



Forward





SECURITY

Create new Lifecycle Workflows

Using the **Azure portal**: template only

Using **Graph API**: start from scratch





SECURITY

Custom task extensions

Lifecycle workflows



Logic Apps



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft



Prepare Logic Apps for LCW

- Trigger + Callback action
- System assigned managed identity
- Authorization policy



SECURITY

When a HTTP request is received

HTTP POST URL `https://prod-132.westeurope.logic.azure.com:443/workflows/2d2bbe18b...`

Request Body JSON Schema

```
{
  "properties": {
    "data": {
      "properties": {
        "callbackUriPath": {
          "description": "CallbackUriPath used for Resume Action",
          "title": "Data.CallbackUriPath",
          "type": "string"
        }
      }
    }
  }
}
```

Use sample payload to generate schema

Add new parameter

Trigger

Where the magic happens

HTTP

* Method

* URI `https://graph.microsoft.com/beta` `Data.CallbackUriPath`

Headers

Queries

Body

```
{
  "data": {
    "operationStatus": "Completed"
  },
  "source": "sample",
  "type": "lifecycleEvent"
}
```

Cookie

Authentication

* Authentication type

* Managed identity

Audience

Callback





Demo time!

- Create new workflow from template
- Extend workflow with Logic Apps



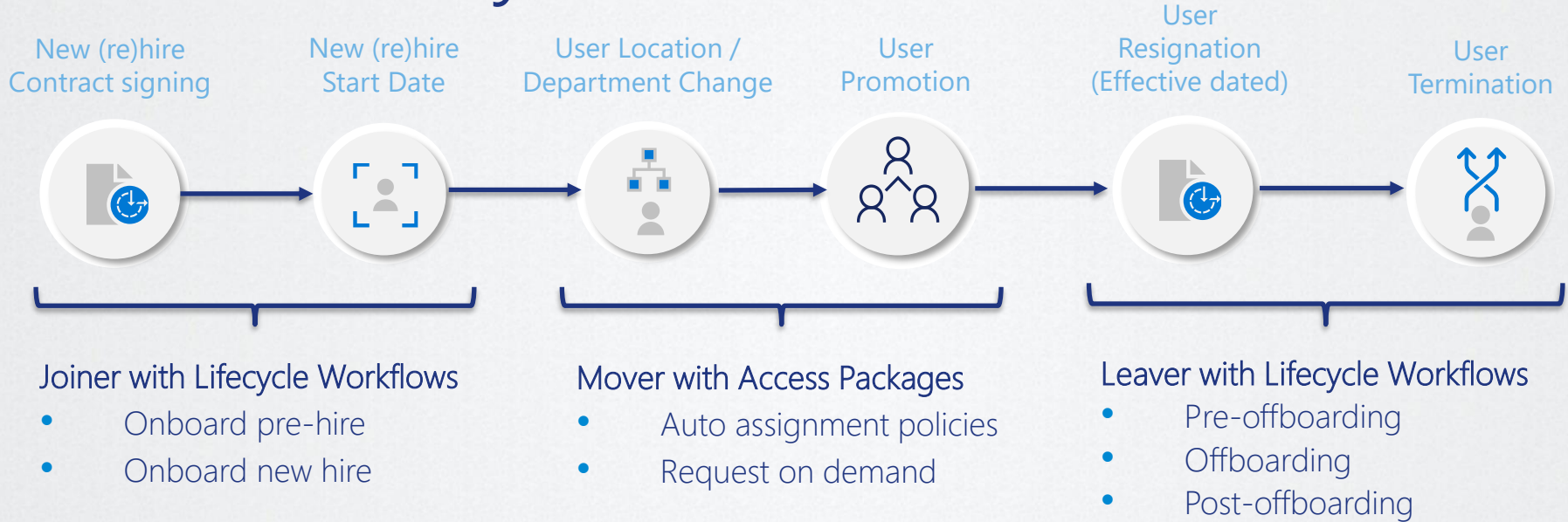


SECURITY

Mover Process



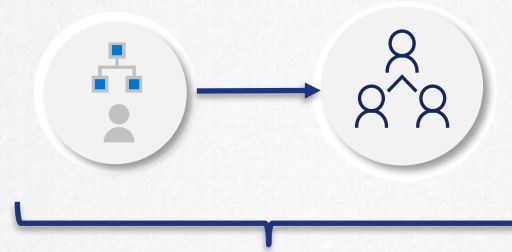
Lifecycle Workflows



Lifecycle Workflows

User Location /
Department Change

User
Promotion



Mover with Access Packages

- Auto assignment policies
- Request on demand





SECURITY

Create Access Packages



- Teams
- Groups
- Applications
- SharePoint sites

Access Package + Approval



- Periodic reviews
- Self-review
- Recommendations

Access Review



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft

Start simple

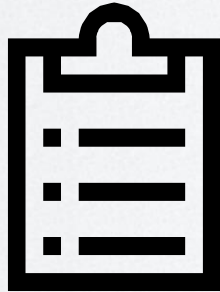


For example:

- Licenses for Visio or PowerBI Pro
- Access to 3rd party apps like Salesforce
- Software within Microsoft Endpoint Manager
- Access to teams with sensitive data



Separation of Duties



Deny access based on:

- Current group membership
- Incompatible Access Packages

Examples:

- Update rings (Fast vs. Slow ring)
- License groups





SECURITY

Policies



Who can request?

- Members and/or guests

Assignments

- Admin assignment (manual)
- On demand (user can request)
- Dynamic assignment (attribute based)





Demo time!

- Access Packages & Reviews
- Create auto assignment policy



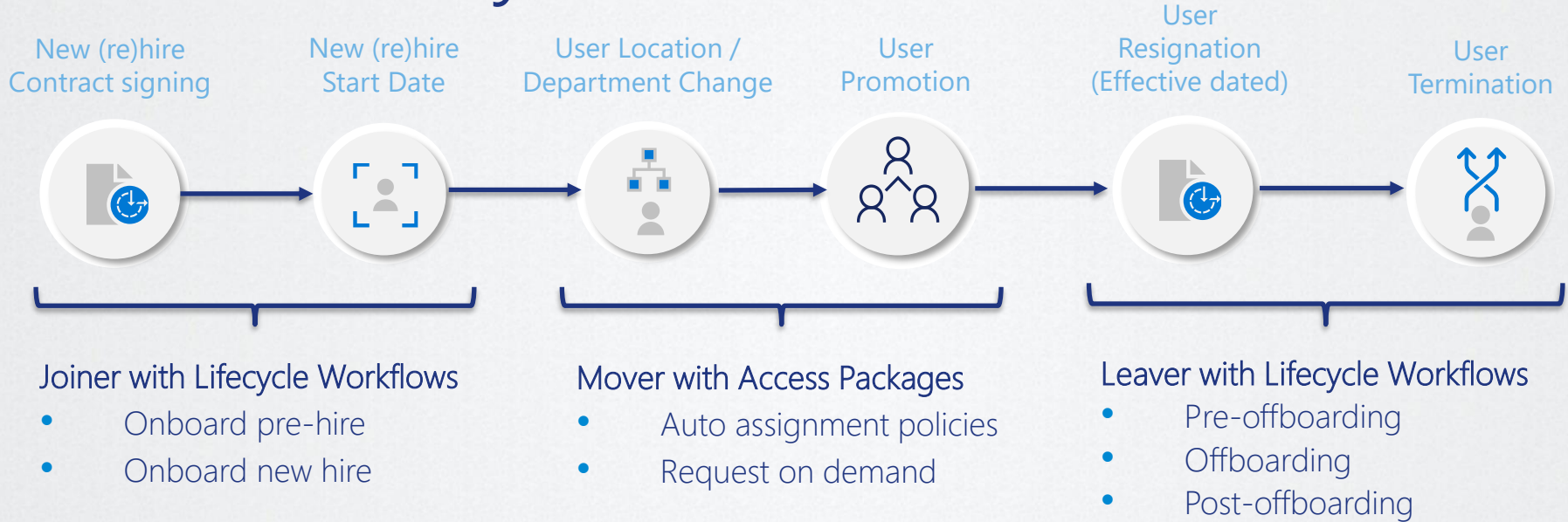


SECURITY

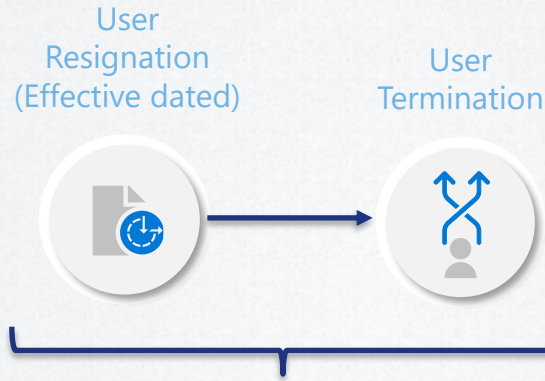
Leaver Process



Lifecycle Workflows



Lifecycle Workflows



Leaver with Lifecycle Workflows

- Pre-offboarding
- Offboarding
- Post-offboarding



Lifecycle Workflows

Available workflow templates for joiners:

 Leaver  On-demand

Real-time employee termination

Execute real-time termination tasks for employees on their last day of work

[Select](#) | [Details](#)

 Leaver

Offboard an employee

Configure offboarding tasks for employees on their last day of work

[Select](#) | [Details](#)

 Leaver

Pre-Offboarding of an employee

Configure pre-offboarding tasks for employees before their last day of work

[Select](#) | [Details](#)

 Leaver









Post-Offboarding of an employee

Configure offboarding tasks for employees after their last day of work

[Select](#) | [Details](#)



Tasks

-  Send email before user's last day
-  Send email on user's last day
-  Send email after user's last day
-  Disable User Account
-  Remove all licenses for user
-  Remove user from all / selected teams
-  Remove user from all / selected groups
-  Run custom task extension



Bunny Bravo verlaat de organisatie vandaag



Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>

Aan: Pim Jacobs



Bunny Bravo verlaat de organisatie vandaag.

Hallo Pim Jacobs,

Uw teamlid Bunny Bravo, is gepland om de organisatie vandaag te verlaten,
9/2/2022.

Uw organisatie heeft het offboarding-proces gestart en er zijn al specifieke acties gepland om het offboarding-proces te voltooien. Met deze acties wordt de toegang tot bedrijfsbronnen, zoals groepen en Microsoft 365 Teams, verwijderd en kan Bunny zich mogelijk niet meer aanmelden.

Als u vragen hebt, neemt u contact op met HR of uw beheerder.

Deze e-mail wordt gegenereerd op basis van een niet-bewaakte alias. Beantwoord niet.

[Privacyverklaring](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

[Beantwoorden](#)[Doorsturen](#)

SECURITY

GET beta <https://graph.microsoft.com/beta/users/stenn.jacobs@jacobsaa.nl>

Request body Request headers Modify permissions (preview) Access token

OK - 200 - 124ms

Response preview Response headers Code snippets Toolkit component Adaptive cards

```
"employeeHireDate": "2022-09-01T01:00:00Z",  
"employeeLeaveDateTime": null,  
"employeeType": null,
```

PATCH beta <https://graph.microsoft.com/beta/users/stenn.jacobs@jacobsaa.nl>

Request body Request headers Modify permissions (preview) Access token

```
{  
  "employeeHireDate": "2022-09-01T01:00:00Z",  
  "employeeLeaveDateTime": "2022-10-01T01:00:00Z"  
}
```





Seeing is believing

- Create offboarding workflow
- Run offboarding workflow
- See results 😊!





SECURITY

Considerations & next steps





SECURITY

Important attributes

Make sure that:

- EmployeeHireDate
- EmployeeLeaveDateTime
- Manager



are populated and synced to Azure AD.





SECURITY

Rome wasn't built in a day



Start out simple
and basic, **but with
a plan!**



Lifecycle Workflows



Access Packages



Access Reviews



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

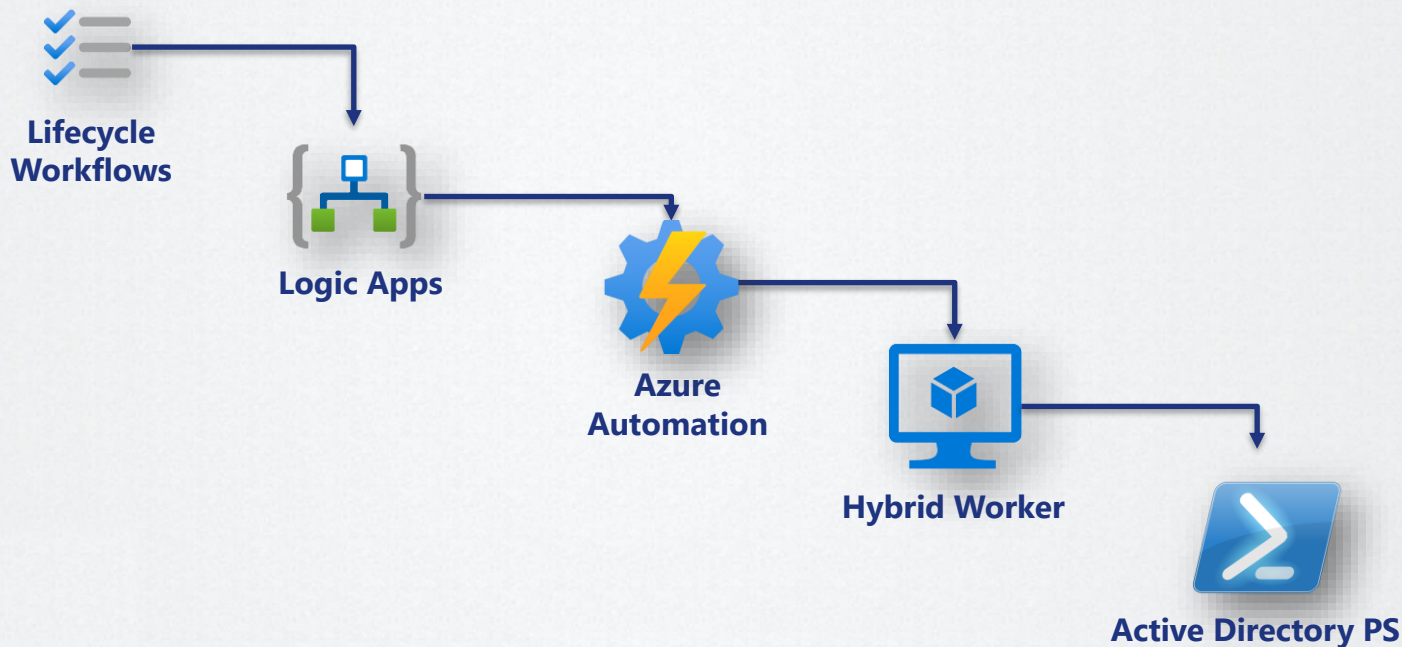
INSPARK

Microsoft



SECURITY

Options for Hybrid Identities



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

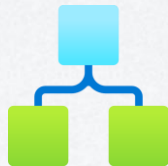
Microsoft



SECURITY



Logic Apps



Start with templates and fill the gaps with Logic Apps to provide hybrid support and custom/complex tasks.



Zero Trust!



Lifecycle Workflows Administrator



Users in this role can create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Azure AD. This role also grants the ability to check the execution of scheduled workflows, launch on-demand workflow runs, and inspect workflow execution log.





SECURITY

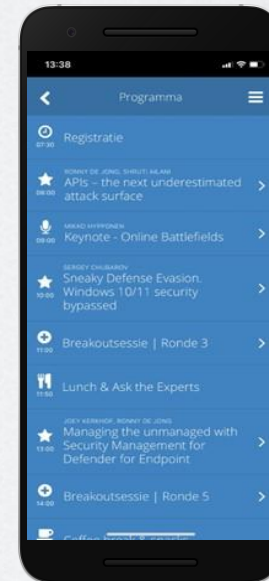
Questions ?






SECURITY

Thank you!



Pim Jacobs 
Principal Consultant
InSpark



Jan Bakker 
Microsoft 365 consultant
Jan Bakker consulting

