User Account Flow
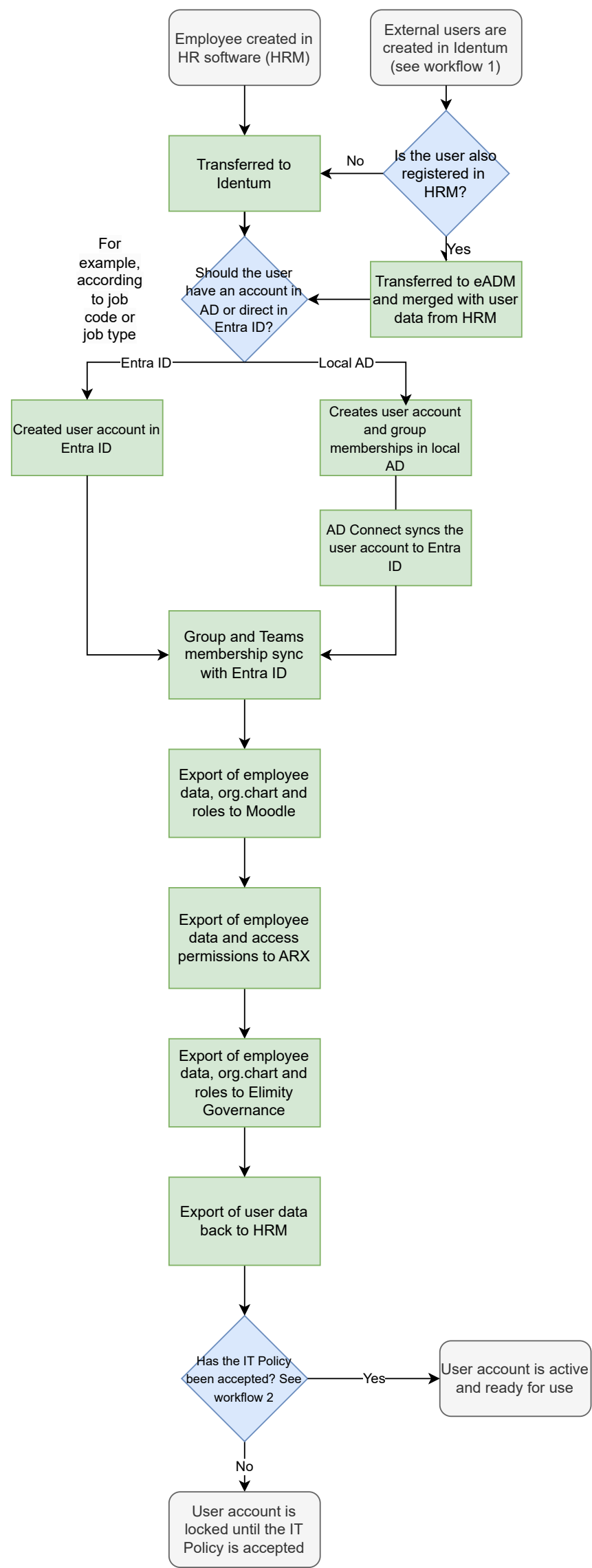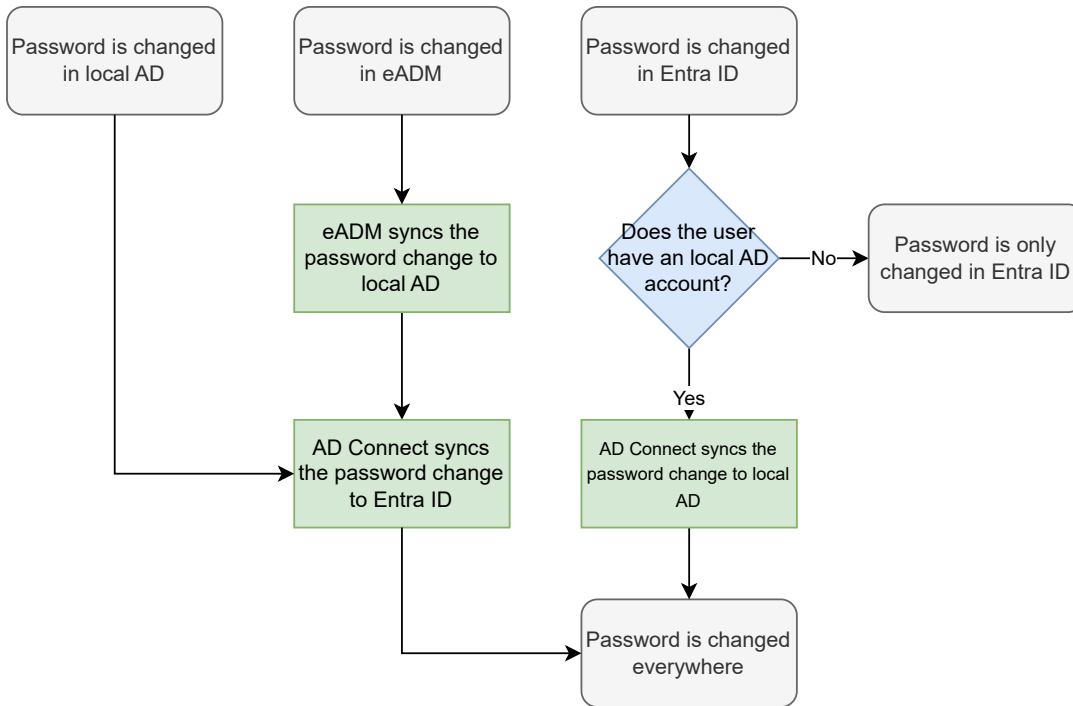
Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.
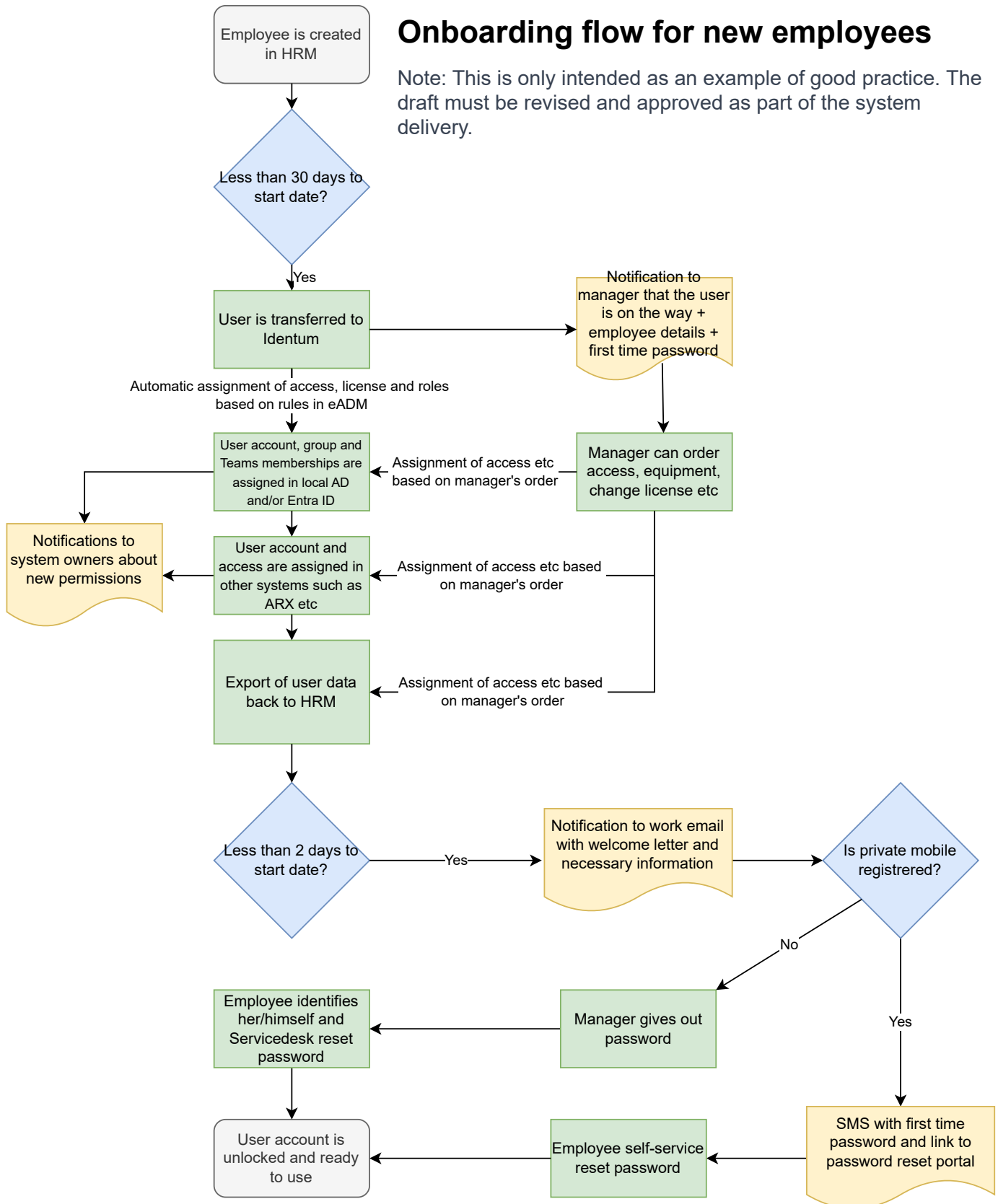
```
┌─────────────────┐          ┌─────────────────┐
│ Employee created │          │ External users are │
│ in HR software   │          │ created in Identum │
│ (HRM)            │          │ (see workflow 1)  │
└────────┬─────────┘          └────────┬─────────┘
         │                             │
         │                        ◇ Is the user also
         │         No             registered in HRM?
         └────────────────────────◇
         │                             │ Yes
┌────────▼─────────┐                   ▼
│ Transferred to   │          ┌─────────────────┐
│ Identum          │          │ Transferred to   │
└────────┬─────────┘          │ eADM and merged  │
         │                    │ with user data   │
For example,                  │ from HRM         │
according to                  └────────┬─────────┘
job code or    ◇ Should the user        │
job type       ◇ have an account in ◄───┘
               ◇ AD or direct in
                 Entra ID?
```

For example, according to job code or job type

Should the user have an account in AD or direct in Entra ID?

- Entra ID → Created user account in Entra ID
- Local AD → Creates user account and group memberships in local AD

AD Connect syncs the user account to Entra ID

Group and Teams membership sync with Entra ID

Export of employee data, org.chart and roles to Moodle

Export of employee data and access permissions to ARX

Export of employee data, org.chart and roles to Elimity Governance

Export of user data back to HRM

Has the IT Policy been accepted? See workflow 2

- Yes → User account is active and ready for use
- No → User account is locked until the IT Policy is accepted

Passwordflow

```
┌────────────────┐    ┌────────────────┐    ┌────────────────┐
│ Password is    │    │ Password is    │    │ Password is    │
│ changed in     │    │ changed in     │    │ changed in     │
│ local AD       │    │ eADM           │    │ Entra ID       │
└───────┬────────┘    └───────┬────────┘    └───────┬────────┘
        │                     │                     │
        │                     ▼                     ▼
        │            ┌────────────────┐         ◇ Does the user ◇      ┌────────────────┐
        │            │ eADM syncs the │        ◇ have an local AD ◇──No──▶│ Password is only │
        │            │ password change│         ◇   account?   ◇        │ changed in Entra │
        │            │ to local AD    │          ◇            ◇         │ ID             │
        │            └───────┬────────┘              │                  └────────────────┘
        │                    │                      Yes
        │                    ▼                      ▼
        │            ┌────────────────┐    ┌────────────────┐
        └───────────▶│ AD Connect     │    │ AD Connect     │
                     │ syncs the      │    │ syncs the      │
                     │ password change│    │ password change│
                     │ to Entra ID    │    │ to local AD    │
                     └───────┬────────┘    └───────┬────────┘
                             │                     │
                             │                     ▼
                             │            ┌────────────────┐
                             └───────────▶│ Password is    │
                                          │ changed        │
                                          │ everywhere     │
                                          └────────────────┘
```
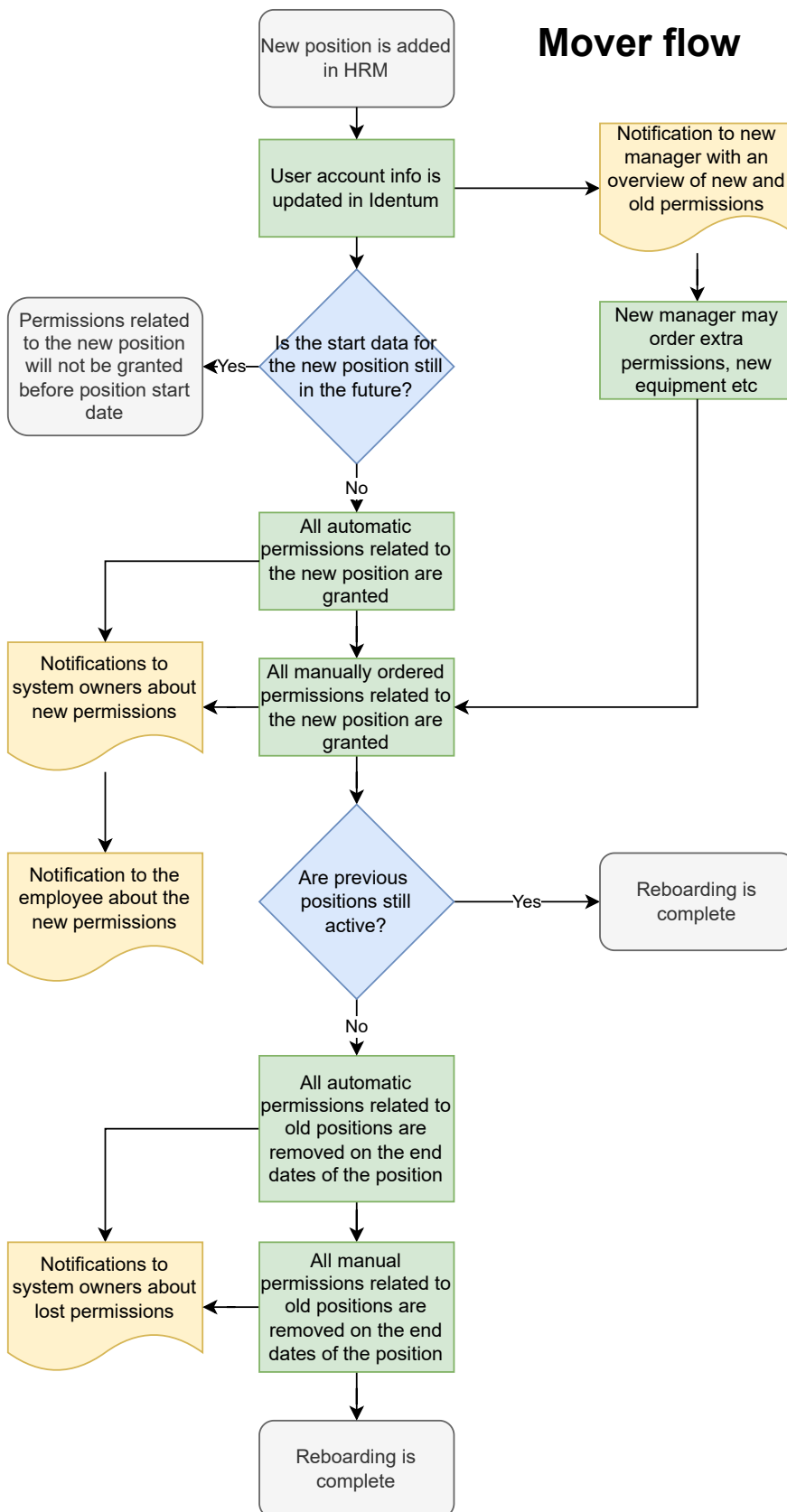
Onboarding flow for new employees

Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.
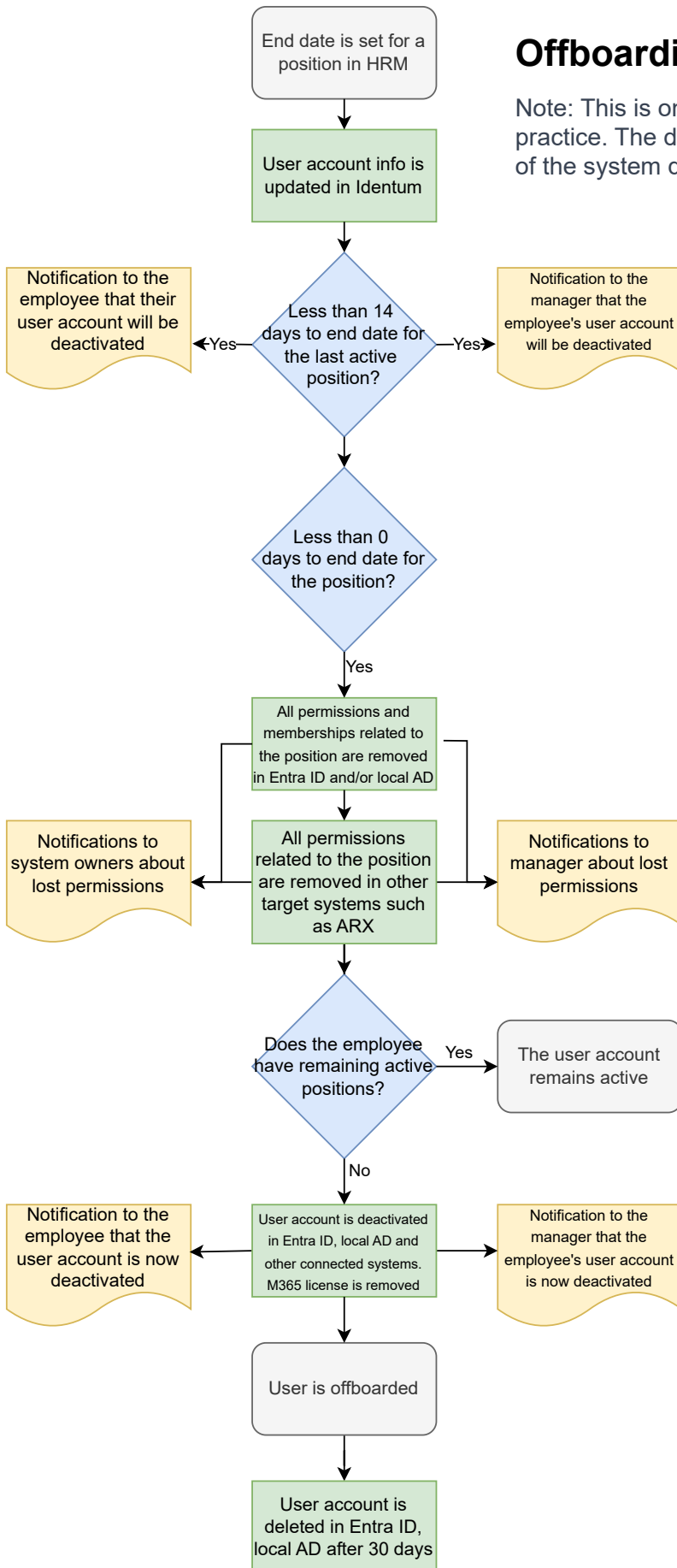
Employee is created in HRM

Less than 30 days to start date?

Yes

User is transferred to Identum

Notification to manager that the user is on the way + employee details + first time password

Automatic assignment of access, license and roles based on rules in eADM

User account, group and Teams memberships are assigned in local AD and/or Entra ID

Assignment of access etc based on manager's order

Manager can order access, equipment, change license etc

Notifications to system owners about new permissions

User account and access are assigned in other systems such as ARX etc

Assignment of access etc based on manager's order

Export of user data back to HRM

Assignment of access etc based on manager's order

Less than 2 days to start date?

Yes

Notification to work email with welcome letter and necessary information

Is private mobile registrered?

No

Manager gives out password

Yes

Employee identifies her/himself and Servicedesk reset password

SMS with first time password and link to password reset portal

User account is unlocked and ready to use

Employee self-service reset password

Mover flow

Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.

New position is added in HRM

User account info is updated in Identum

Notification to new manager with an overview of new and old permissions

New manager may order extra permissions, new equipment etc

Is the start data for the new position still in the future?

Yes — Permissions related to the new position will not be granted before position start date

No

All automatic permissions related to the new position are granted

Notifications to system owners about new permissions

All manually ordered permissions related to the new position are granted

Notification to the employee about the new permissions

Are previous positions still active?

Yes — Reboarding is complete

No

All automatic permissions related to old positions are removed on the end dates of the position

Notifications to system owners about lost permissions

All manual permissions related to old positions are removed on the end dates of the position
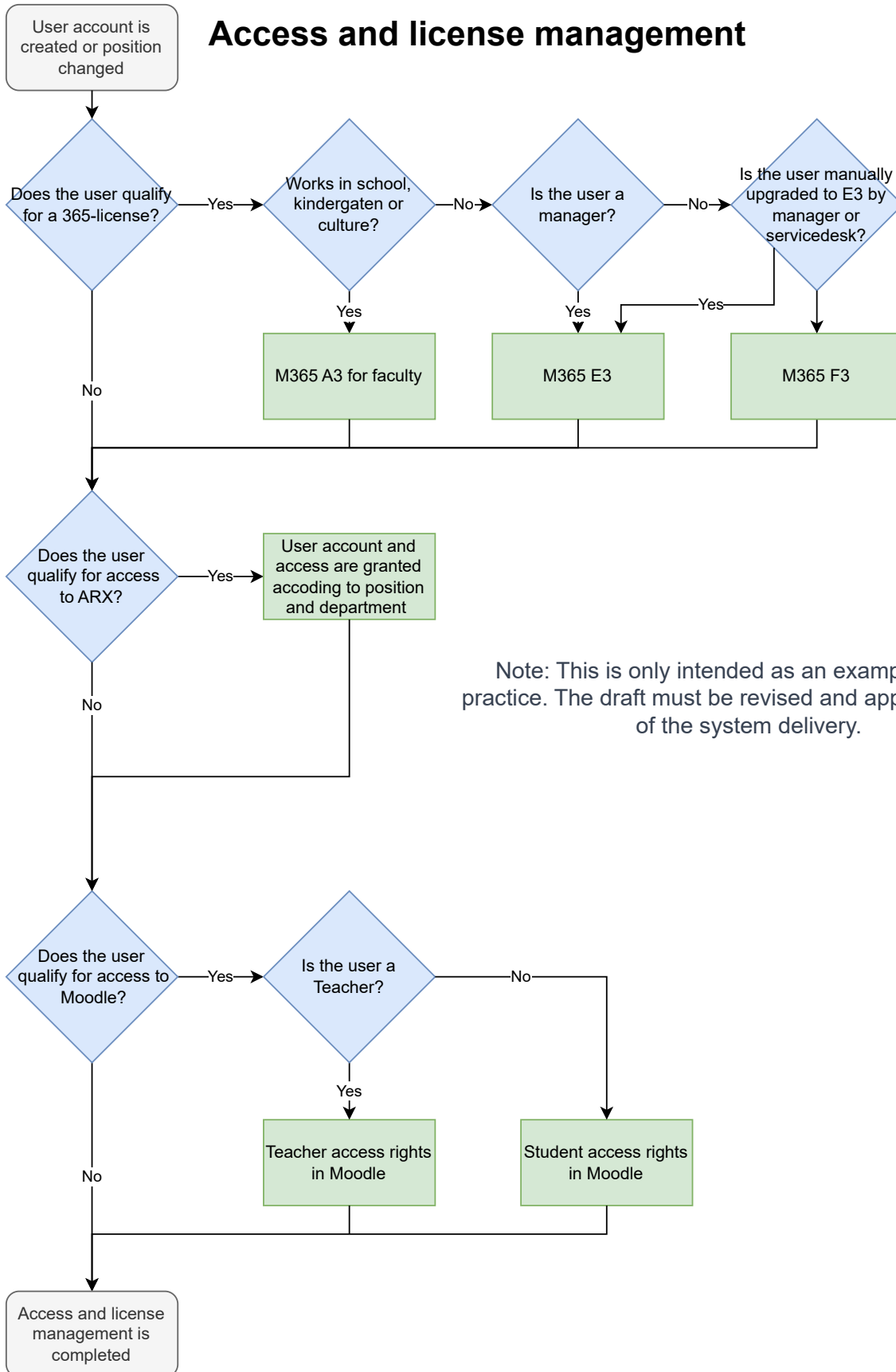
Reboarding is complete

Offboarding flow

Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.
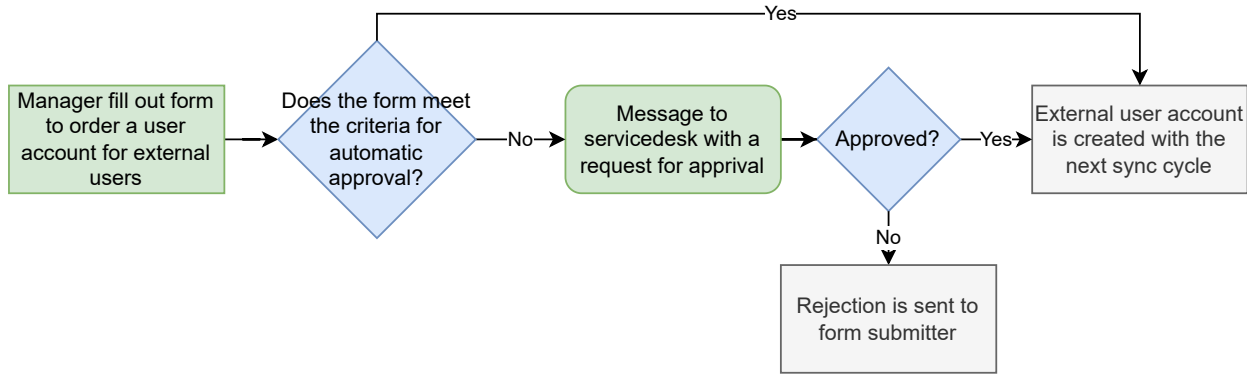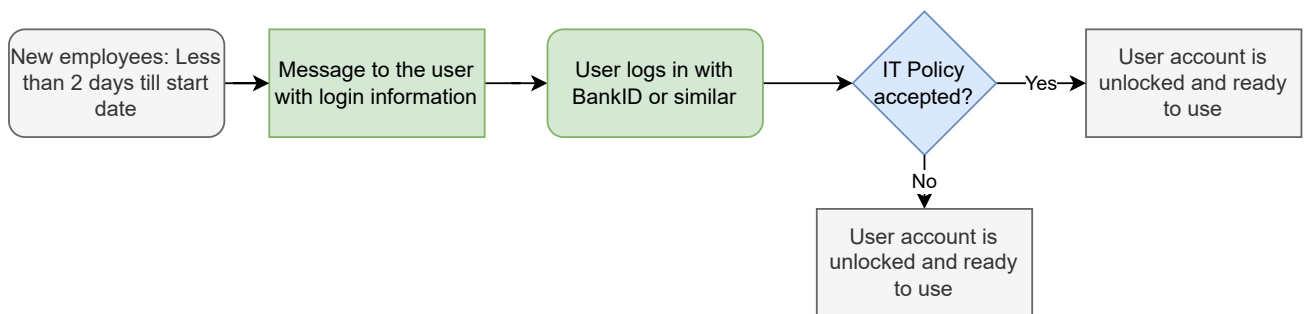
```
End date is set for a
position in HRM
        │
        ▼
User account info is
updated in Identum
        │
        ▼
Less than 14 days to end date for the last active position?
  ◄─Yes── Notification to the employee that their user account will be deactivated
  ──Yes─► Notification to the manager that the employee's user account will be deactivated
        │
        ▼
Less than 0 days to end date for the position?
        │ Yes
        ▼
All permissions and memberships related to the position are removed in Entra ID and/or local AD
        │
        ▼
All permissions related to the position are removed in other target systems such as ARX
  ◄──── Notifications to system owners about lost permissions
  ────► Notifications to manager about lost permissions
        │
        ▼
Does the employee have remaining active positions?
        ──Yes──► The user account remains active
        │ No
        ▼
User account is deactivated in Entra ID, local AD and other connected systems. M365 license is removed
  ◄──── Notification to the employee that the user account is now deactivated
  ────► Notification to the manager that the employee's user account is now deactivated
        │
        ▼
User is offboarded
        │
        ▼
User account is deleted in Entra ID, local AD after 30 days
```

Access and license management

User account is created or position changed

Does the user qualify for a 365-license? —Yes→ Works in school, kindergaten or culture? —No→ Is the user a manager? —No→ Is the user manually upgraded to E3 by manager or servicedesk?

No (from first decision)

Yes → M365 A3 for faculty

Yes → M365 E3

Yes → M365 E3

Yes → M365 F3

Does the user qualify for access to ARX? —Yes→ User account and access are granted accoding to position and department

No

Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.

Does the user qualify for access to Moodle? —Yes→ Is the user a Teacher? —No→ Student access rights in Moodle

Yes → Teacher access rights in Moodle

No

Access and license management is completed

Note: This is only intended as an example of good practice. The draft must be revised and approved as part of the system delivery.

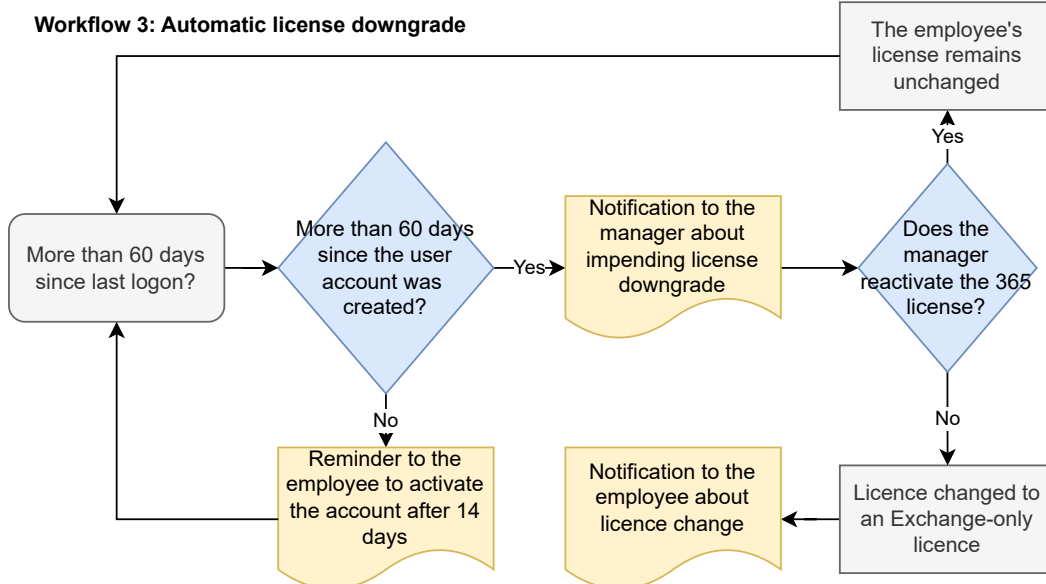**Workflow 1: Order form for external users**

Manager fill out form to order a user account for external users → Does the form meet the criteria for automatic approval? —No→ Message to servicedesk with a request for apprival → Approved? —Yes→ External user account is created with the next sync cycle

Does the form meet the criteria for automatic approval? —Yes→ External user account is created with the next sync cycle

Approved? —No→ Rejection is sent to form submitter

Workflow 2: IT policy for new users

New employees: Less than 2 days till start date → Message to the user with login information → User logs in with BankID or similar → IT Policy accepted? —Yes→ User account is unlocked and ready to use

IT Policy accepted? —No→ User account is unlocked and ready to use

Workflow 3: Automatic license downgrade

More than 60 days since last logon? → More than 60 days since the user account was created? —Yes→ Notification to the manager about impending license downgrade → Does the manager reactivate the 365 license? —Yes→ The employee's license remains unchanged

More than 60 days since the user account was created? —No→ Reminder to the employee to activate the account after 14 days

Does the manager reactivate the 365 license? —No→ Licence changed to an Exchange-only licence → Notification to the employee about licence change

Overview for new bees

Masterdata

HRM-system

← write back →

Importfilter

creating Users
checking AD/EntraID

IDENTUM

Rule sets defining **access**,
permissions and
memberships

Cloud / Catalogue

Target systems

Messageflows informing
users, managers and/or
system administrators