GUARD-Prozesse – Evidenzierung (1) –

No.	Cat.	Process	Target	Comment
25	E	Show unknown people (in the IdM system, not on the HR database)	• To identify the missing persons in the HR database and improve the quality of the the HR database data through the IdM system. • To ensure that nobody uses a system without being in the HR database. • To provide management with information about the the HR database data quality.	Core IAM Process
26	E	Show leavers (on Should, not on Belong)	• To identify the open 'Should' records for users who have already left the company. • To improve the quality of the the IdM system data. • To reduce the risk of misuse of unused accounts.	Core IAM Process
27	E	Show mistakes (on Actuality, not on Belong)	• To identify the open system accounts for users who have already left the company. • To improve the quality of the system data. • To reduce the risk of misuse of unused accounts.	Core IAM Process
28	E	Show execution error/hacker (on Actuality, not on Should)	• To ensure that all accounts (access rights), which find their way into a system without going through administration will be detected and could be checked (could be an indication of intruders on the system). • To identify problems with the execution of account deletion and/or removing of authorities.	Core IAM Process

GUARD-Prozesse – Evidenzierung (2) –

No.	Cat.	Process	Target	Comment
29	E	Import data into the Access Rights Evidence including creation of import anomalies	• To ensure that all uploaded person records will be assigned to the right user in the IdM system.	Internal Process
30	E	Check import anomalies manually	• To ensure that all uploaded person records will be assigned to the right user in the IdM system. • To improve the quality of the the IdM system data.	Work Instruction
31	E	Create report	• To support a standardised procedure for the creation of a new report including defined responsibilities and informing the users.	System Functionality
32	E	Modify report	• To support a standardised procedure for the modification of existing reports including defined responsibilities and informing the users.	System Functionality
33	E	Delete report	• To support a standardised procedure for the deletion of existing reports including defined responsibilities and informing the users.	System Functionality

GUARD-Prozesse – Evidenzierung (3) –

No.	Cat.	Process	Target	Comment
34	E	Show information for Requestor	• To show the Requestor his own access rights.	System Functionality
35	E	Show information for Line Manager/ IS Officer	• To support a secure and extensive information facility for 'Line Manager'/'IS Officer'.	System Functionality
36	E	Show information for System Owner/ System Administrator	• To support a secure and extensive information facility for 'System Owner'/'System Administrator'.	System Functionality
37	E	Show information for Audit	• To support a secure and extensive information facility for 'Audit'.	System Functionality
38	E	Show information for Profile Owner	• To support a secure information facility for 'Profile Owner'.	System Functionality
39	E	Show status of a request	• To make it possible for every request workflow-participant to see the status of the request (history and future).	System Functionality

GUARD-Prozesse – Evidenzierung (4) –

No.	Cat.	Process	Target	Comment
40	E	Upload data from Verify to Should	• To ensure that only completely approved requests are treated as Should data.	Internal Process
41	E	Upload data from the systems to Actuality	• To support a standardised procedure for the delivery, normalisation and upload of system access rights data (including upload monitoring and error correction).	Internal Process
42	E	Upload data from the HR database to Belong	• To support a standardised procedure for the delivery, normalisation and upload of reference data (including upload monitoring and error correction).	Internal Process
43	E	Connect a new system to the IdM system	• To support a standardised procedure for the connection of new systems to the IdM system.	Work Instruction
44	E	Remove a system from the IdM system	• To support a standardised procedure for the removal of systems from the IdM system.	Work Instruction

GUARD-Prozesse – Antragsworkflow (1) –

No.	Cat.	Process	Target	Comment
1	W	Administrate unique User-id's	• To ensure that there is nobody using a system, without being recorded in the HR database - (connection between person and 'User'). • To ensure that each 'User' within the IdM system is identifiable by a global unique User-id. • Eliminates separate application for User-ids per system - (one unique User-id is available globally for each person)	Work Instruction
2	W	Create the unique User-id	• To ensure that each 'User' on the system is identifiable by a global unique User-id. • No separate application for unique User-ids. • Each request form must contain a unique User-id. • Each missing unique User-id is created via this process.	Core IAM Process
3	W	Add account	• A formal 'User' registration procedure is a basic security requirement. • To create personal accounts and system accounts via one process.	Core IAM Process
4	W	Delete account	• Deletion of 'User' accounts, which are not necessary for User's job. • To delete personal accounts and system accounts via one process.	Core IAM Process
5	W	Delete User	• Timely deletion of all 'User' accounts for 'employees' (internal and external) who have left the company.	Core IAM Process

GUARD-Prozesse – Antragsworkflow (2) –

No.	Cat.	Process	Target	Comment
6	W	Change name	• ‘User’ names are up to date in all relevant systems. • For correct referencing across Systems and Databases consistent updates of ‘User’ names are of paramount importance. • Every name change of any ‘User’ has to be maintained via this process. • There is no manual request for changing the name allowed. Only name changes in the HR database will trigger this process automatically.	Core IAM Process
7	W	Change account name	• To support a process of changing account names for name based accounts, without loosing access rights or ‘User’ data. • Each account name change has to be maintained via this process. • There is no automatic request for changing the account name allowed.	Core IAM Process

GUARD-Prozesse – Antragsworkflow (3) –

No.	Cat.	Process	Target	Comment
8	W	Change department	• To ensure all accounts have proper authorisation. • To ensure department code for ‘employee’ is valid at all times. • To ensure both departments (old and new) take part in the department change process. • To avoid an ‘employee’ having inappropriate access to data from the old department. • All department changes for all ‘employee’s must be maintained via this process. • There is no manual request for changing the department allowed.	Core IAM Process
9	W	Change Department code	• To ensure that an 'update department code mechanism' exists, for all systems, which maintain the department code. • Every department code change of any account has to be maintained via this process. • There is no manual request for changing the department code allowed.	Internal Process

GUARD-Prozesse – Antragsworkflow (4) –

No.	Cat.	Process	Target	Comment
10	W	Change expiry date	• 'User' accounts with an expiry date (mainly external staff) are available only when needed, no shorter and no longer. After the expiry date is reached, the account is automatically disabled by the system itself or manually by the responsible 'System Administrator'. • Every expiry date change of any account has to be maintained via this process. • There is no manual request for changing the expiry date allowed.	Core IAM Process
11	W	Check form	• To ensure requests are completed correctly.	Core IAM Process
12	W	Add access rights	• To ensure that all accounts have proper authorisation. • To maintain also system accounts via this process. • To maintain also changing of special account-information (e.g. system specific fields) via this process. • Assignment of access rights according to the functional needs is a fundamental requirement of security.	Core IAM Process
13	W	Remove access rights	• To ensure that all accounts have proper authorisation. • To maintain system accounts via this process. • To maintain the changing of special account information (e.g. system specific fields). • Deletion of access rights according to functional needs is a fundamental requirement of security.	Core IAM Process

GUARD-Prozesse – Antragsworkflow (5) –

No.	Cat.	Process	Target	Comment
14	W	Enable account	• To restore access rights for a previously disabled ‘User’ account.	Core IAM Process
15	W	Disable account	• Disable ‘User’ accounts without deleting, so they can be restored easily by the enabling process if necessary. • Disable ‘User’ directly after their expiry date in the HR database is reached. • Offer a quick process for disabling, as it is usually a time critical task.	Core IAM Process
16	W	Set password	• Provide a secure and efficient process for password requesting and delivery.	Core IAM Process Has to include Out-of-band Verification for Password Resets

GUARD-Prozesse – Antragsworkflow (6) –

No.	Cat.	Process	Target	Comment
17	W	Inform personnel administration department	• To make it possible to request for access rights for a person who is not as yet in the HR database. • To limit mis-use of User-id's by ensuring 'employee's are only using their own unique User-id and not another employee's id. • Improve the HR database data quality by the IdM system. • It is a main requirement of the IdM system, that every 'User' (internal and external) has to be in the HR database.	Work Instruction
18	W	Recording profile information	• To ensure that new profiles are known by the IdM system. • To ensure that all necessary profile attributes for requesting and for the workflow steering are known by the IdM system. • Each new profile must be recorded in the IdM system via this manual process before the access right is available for request.	System Functionality Core IAM Process Group for Profiles required as for Users
19	W	Modify profile information	• Each modification of profile attributes must be announced in the IdM system via this process, to ensure up to date access rights and workflow steering information.	System Functionality

GUARD-Prozesse – Antragsworkflow (7) –

No.	Cat.	Process	Target	Comment
20	W	Switch profile off	• To ensure that it is no longer possible to request for a deleted profile. • Each deletion of a profile must be announced in the IdM system via this process, to ensure up to date access rights and workflow steering information.	System Functionality
21	W	Break down of the IdM system	• To ensure that the electronic workflow functionality is in place even in case of a the IdM system break down.	Work Instruction
22	W	Emergency route for account deletions	• To ensure that there will be an emergency route for urgent account deletions, without loosing time by waiting for departmental approval. This could be necessary in case of an security incident, suspicion of access rights abuse or if an momentous administration error will be detected.	Core IAM Process
23	W	Emergency route for removal of access rights	• To ensure that there will be an emergency route for urgent removal of access rights, without loosing time by waiting for departmental approval. This could be necessary in case of an security incident, suspicion of access rights abuse or if an momentous administration error will be detected.	Core IAM Process
24	W	Maintenance of the IdM system access rights		Work Instruction