Meeting Date: Wednesday 9th March

Attendees: Lee Collins (LC), John Green (JG), Tom Greenwood (TG), Steve Harrison (SH), Mark Hilditch (MH), Stuart Ogden (SO) Note-taker, Angus Rae (AR), Paul Robinson (PR), Wayne Tomkinson (WT),   
Cherylea Towers (CT),

**Background:**

Following the enforced password policy for Staff in early February, attention now switches to realising the change to the policy for Students. The meeting was scheduled to bring together stakeholders to discuss options available and to agree on an approach that introduces the policy in a sensible way to minimise impact.

**Summary Information:**

* The password policy was updated in March 2015, under RFC685
* Accounts created, or had a password change since March 2015 are subject to a policy with increased complexity, but not password ageing.
* Accounts created prior to policy change in March 2015, nor reset their password since are still being managed by the old policy. Essentially this applies to many 2nd and 3rd year student accounts.
* The impact of enforcing a password change on accounts that don’t comply with new policy would be significant. Approximately 16,500 accounts have logged in within the past 180 days, but have a password older than 180 days. (further details see TG’s embedded document)  
  
* The volume of calls from staff to the Service Desk following the enforced policy increased by 33%
* Communication to students has been limited to screen pop-ups, the current pop-up doesn’t emphasise a deadline for the student to update their password.  
  

**Decision’s reached:**

1. The priority is to demonstrate progress to address the password policy issue.
2. Demonstrating progress should be balanced against the impact the change is likely to have. As such, enforcing the policy over the Easter break will be deferred.
3. The potential impact of enforcing policy change to an account for a student in their final year outweighs the benefit. These accounts will reduce naturally as they move through the lifecycle. No Action required.
4. A phased approach to introducing policy changes for complexity.
   1. Students starting as Year 1 in September 2016 will be provisioned with complexity and ageing rules (Action2)
   2. Students returning as Year2 in September 2016 will already have complexity set.
   3. ITS will encourage Students returning as Year 3 in September 2016 to reset their password, but will enforce the policy on 1st August 2016. Policy will enforce complexity and ageing at the same time.
5. A phased approach to introducing ageing will be applied to Students returning as Year2.
6. Ageing will be set to 12 months for students. Staff will remain on 6 months.
7. The aim is to have completed the work during 2016.

Action Log:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Action Ref** | **Action Area** | **Description** | **Suggested Owner** | **Update** | **Status** |
| 1) | AD | Create an AD Group that enforces the strengthened complexity and ageing password policy rules to students. | TG |  |  |
| 2) | AccMan Update | Change to AccMan scripts relating to the provisioning of new student accounts. On provisioning of a student, the account should be created and added to the AD group described in Action 1.  Ensures 2016 Year1 student accounts are created as per the desired policy. Preventing the problem from growing any further. | SH | Alter transaction 93, ACTIVE\_DIRECTORY\_NEW\_USER to add user to new group. | 1-3 days |
| 3) | AccMan / Password Self Service | Change to AccMan scripts following a self-service AD password reset.  On initiating a self-service password change, the account should be added to the AD group described in Action 1.  Introduces complexity and ageing rules on a random basis for current students, will lessen the impact of enforced complexity and ageing rule for returning 2nd / 3rd year students. Should be actioned as soon as practical. | SH | Amend transaction 91, SET\_USER\_ACTIVE\_DIRECTORY\_PASSWORD to add user to new group.  **Validate old passwords**  Password Reset does not enforce verification against the last 15 passwords. To enforce this we would need to store hashes of each AD password generated in the Accman database. The hashes can be matched against the user entered password so the SET\_USER\_ACTIVE\_DIRECTORY\_PASSWORD transaction does not fail. | 1-3 days  2-4 days |
| 4) | AccMan  Update | Change to AccMan scripts used when a Service Desk agent resets a student’s AD password.  Following Service Desk resetting students AD password, the account should be added to the AD group described in Action 1. | SH | Amend Accman FE to include Password Reset style validation (See Action Ref 3 - Validate old passwords).  The change to the password is done by transaction 91 (See Action Ref 3). | 2-5 days  0 days |
| 5) | Process / Communication | Following completion of Actions 3&4, Service Delivery to continue with communication to encourage students to reset passwords.  With a view that this will ramp up towards the summer break and an enforced password change on 1st August 2016 for students who will return as 3rd Year in September 2016.  Communications to include   1. Update Screen Pop-Up 2. Email and Student pages updates via Student News 3. Talk to School Ops managers for local cascade. | SO |  |  |
| 6) | AD/AccMan | Identify cohort of students who will return as 3rd year in September 2016, and who are not subject to complex policy and ageing rules.  With a view to adding them on mass or on a phased basis to the AD group created in Action 1. | tbc | Possibly one-off SQL/PowerShell script. |  |
| 7) | AD | Identify cohort of returning 2nd year students who do not have ageing rules in place. Introduce ageing on following completion of Registration on a phased basis. | TG |  |  |