ISC10D021

Password Disclosure

The following paper provides background on the way in which incidents of password disclosure are handled by ISD: the process has been designed to match the policy agreed in the Conditions of Computer Use. Disclosure of passwords by staff or students can have serious consequences for the University as it can lead to blacklisting by external email providers.

Points 9 – 12 of the Process for handling password disclosures section outlines the process that is followed for second and subsequent offences.

The committee should be aware that the implication of adopting the processes outlined here is that there will be an inevitable delay in reinstating access to IT services, which may prove very inconvenient for those people who continue to reveal their passwords after they have received an initial warning.

We seek confirmation from ISSC that this is a reasonable approach.

Processes for Password Disclosure Incidents
Detection, recording, handling and referring on

Document control information

Title:	Dealing with Password Disclosure Incidents
Date:	28 January 2011
Version:	V1.3
Reference:	IS-SPC/PWPROC/DRAFT/V1.3
Authors:	Steve Mosley
Quality Assurance:	ISDMT – Approved xxxxx

Scope

This document details how detected password disclosures by users should be recorded as incidents and how they should be subsequently handled and where appropriate passed on for further action. Some background information is also given on how password disclosures are detected and the immediate measures that are taken to block them.

Technical detail on detection and blocking mechanisms and detail of how incidents are logged and tracked on the ESD Helpdesk system are not included

Detection and blocking of password disclosures

Password disclosures are detected via three main routes:

1. **Compromised UEA IT accounts which are sending out spam emails** (i.e. user's password has been successfully compromised by a party external to UEA).
   Spam emails being sent from compromised IT accounts are detected from monitoring of Canit spam filtering system logs and webmail server logs. Where compromised UEA IT accounts have been detected sending out Spam, access to email by that account is immediately blocked, so as to prevent further transmission of spam emails from that account. An email is sent to the Helpdesk to request that the IT account is disabled. The compromised IT account is not always as a result of a user responding to a phishing email, but can also be caused by malware infection of the user's computer e.g. trojans/key loggers.
2. **Traps setup in Canit for known phishing email sender addresses**
   Users have attempted to send their password within an email to a known phishing email address. Note, the user has not successfully disclosed their password to an external party, only to staff monitoring the trap.
3. **Traps setup on the DNS for known phishing web sites**
   These traps redirect users attempting to connect to a phishing web site to a 'dummy' UEA web page. The dummy web page contains a form on which the user's username and password are requested. If the user responds, their username and password are sent to staff monitoring the trap (but are not revealed to an external party).

Process for handling password disclosures

Note, some of the steps below are already in place (e.g. 1 and 2), but not formally documented. Other steps in the process are what is proposed based on discussions with the User Services Manager (Cath Baker), the Senior Helpdesk Advisor (Dudley Beckles) and with staff who currently monitor for password disclosures.

1. Monitoring staff detect password disclosures by means described in the previous section 'Detection and blocking of password disclosures' .
2. If the user's password has been successfully disclosed to parties external to UEA (route 1 in the previous section), then the System Specialist responsible for email gateways, or the Duty Ops immediately disable the user's access to email. They should also search for the text "password" in the sent mail folder for the offending account, in order to gather evidence of the user having emailed their password to an external party.
3. Monitoring staff email the Helpdesk requesting that they disable the user's IT account in SPOT. If evidence was found in step 2 of the user having emailed their password, this should also be sent to the Helpdesk.
4. The Helpdesk disables the user's IT account in SPOT and creates an entry on the Helpdesk system. They check their records to see whether the user has previously disclosed their password within the preceding 12 months.
5. The user on discovering that their account is not operational contacts the Helpdesk who informs them why the account has been disabled and draws their attention to:
    - The Conditions of Computer Use (CoCU) - password disclosures are referred to in the summary points and in 3.4j of 'Unacceptable Use'.
    - The consequences for the user i.e. someone else has access to their account and email.
    - The consequences for the University of their password being disclosed – blacklisting of UEA by external ISPs.
    - Educational material regarding on-line safety[1]
6. If the disclosure was detected via spam from a compromised IT account (route 1 in previous section) and the user denies that they have disclosed their password to anyone else, and there is no evidence from searches of their sent mail folder of them having emailed their password, then it should be assumed that their computer has been compromised by a Trojan or key logger. If they have been using a personally owned computer (e.g. student in residences), they should be advised to scan with anti-virus/anti-malware software to remove any malware. If they have been using a UEA owned computer, then the relevant IT support staff should be requested to inspect the machine for malware and take whatever measures necessary to ensure it is no longer infected. Once the machine is deemed to be 'clean' the user or IT support, whichever is appropriate, should inform the Helpdesk so that they can re-enable the account as in step 7 and close the Helpdesk call.
7. If this is a first offence, the Helpdesk then re-enables the user's account on SPOT and informs the email gateways Systems Specialist and the Duty Ops to re-enable the user's access to email if this has been disabled. The re-enablement process on

[1] The educational material relevant to this and other types of insecure behaviour on the network and internet should be reviewed by User Services on a regular basis, at least annually.

SPOT involves giving the user a new default password which they have to change at their first login.

8. If this is a first offence, the Helpdesk follows up the account re-enablement by sending an email to the user :
    - Confirming that their account has been re-enabled
    - Re-iterating the verbal warning already given to the user
    - Warning them that should they be detected disclosing their password on a subsequent occasion, their account will be disabled without further warning and the matter referred to the appropriate authority for further action to be taken
    - Making them aware of 3.4j under 'Unacceptable Use' in the CoCU re. non-disclosure of passwords
9. Should this be a 2nd/ subsequent offence, the Helpdesk informs the user that the matter is being referred and they email misuse@uea.ac.uk[2] giving details of the incident and user.

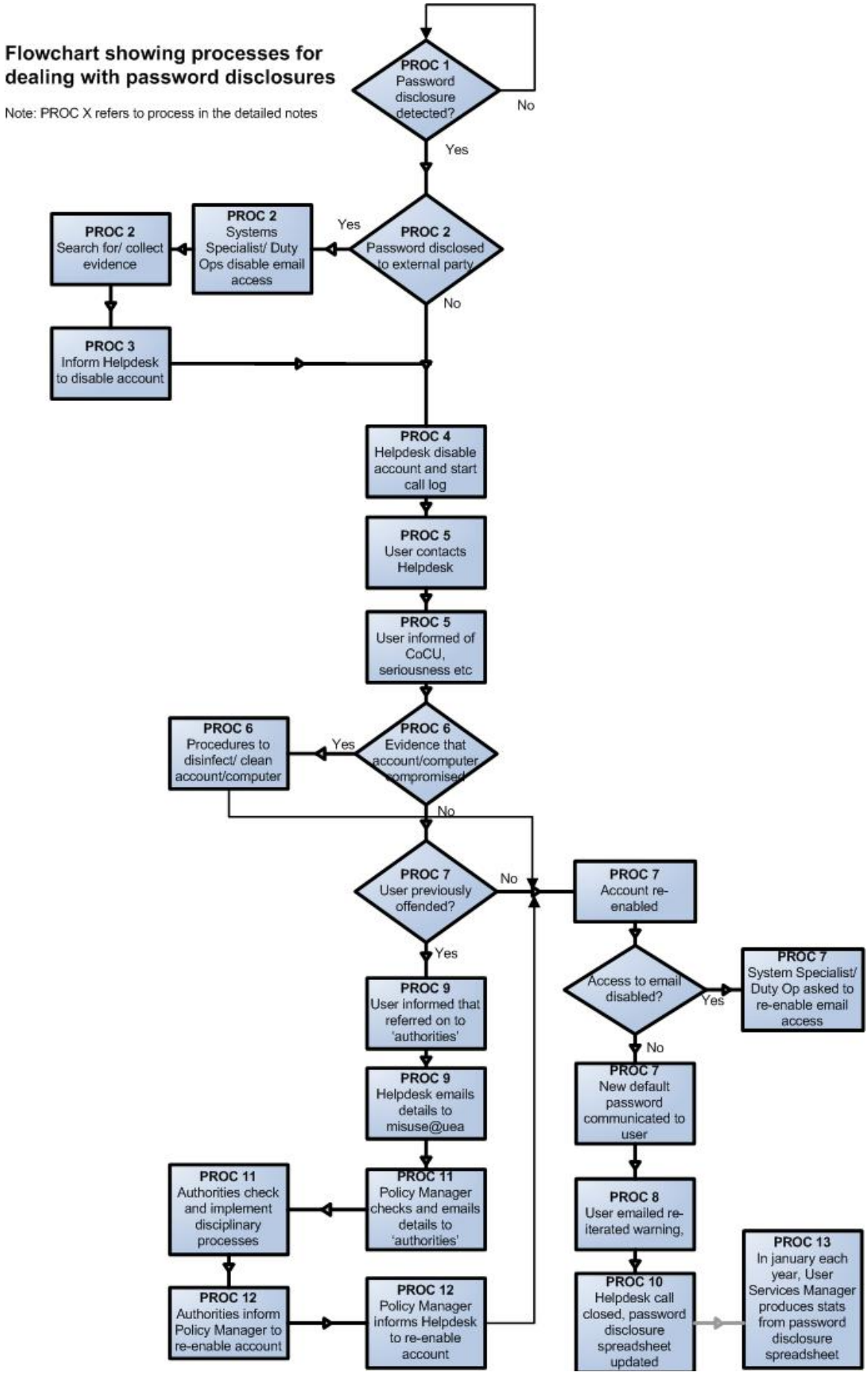
    If the user asks who can they contact to discuss the matter with, they are directed to the appropriate authority (see 11)
10. The Helpdesk record details on the Helpdesk system of email communications with the user and actions taken. They also record details on the separate 'password disclosure incident' spreadsheet .
11. On receiving the email to misuse@uea, the ICT Policy Manager checks the details and refers the matter to the appropriate authority. For staff this is the relevant HR Manager. For UEA students it is the Senior Resident Tutor. For INTO students it is the Head of INTO Student Services and the INTO Student Services Manager. These people determine any further disciplinary action that should be taken and contact the appropriate people to progress this. Current contact details for these people are listed in the appendix to this document.
12. The HR Manager/ Senior Resident Tutor/ Head of INTO Student Services as appropriate, inform the ICT Policy Manager (or deputy) when the offender's IT account can be re-enabled. The ICT Policy Manager informs the Helpdesk (email to staff.help@uea?) to re-enable the IT account and close the call following procedures as in step 7 and 10.
13. At the end of January each year the User Services Manager (Cath Baker) will produce a spreadsheet report for the ICT Policy Manager giving details about password disclosure incidents including the total number of incidents processed during the just ended calendar year (1st Jan to 31st Dec), the number of repeat offences and the change on the previous year. The ICT Policy Manager will incorporate this information into misuse/abuse statistics for the Director of IS to report to the Spring meeting of ISSC.

Below is a flowchart providing a summary view of the above documented processes.

[2] The misuse@uea email address directs the email to the ICT Policy Manager (Steve Mosley), Raymond Scott (Deputises for ICT Policy Manager when absent) and to the Director of Information Services, Jonathan Colam-French (for information only).

Flowchart showing processes for dealing with password disclosures

Note: PROC X refers to process in the detailed notes



Appendix

Referral contacts

HRD

Jenny Evans, HR Manager Central Divisions, Tel. x2124, Email Jenny.Evans@uea.ac.uk
Alison Clements, HR Manager SCI, Tel. x2193, Email Alison.Clements@uea.ac.uk
Linda Cole, HR Manager HUM, Tel. x3582, Email Linda.Cole@uea.ac.uk
Santha Forder, HR Manager SSF, Tel. x2936, Email S.Forder@uea.ac.uk
Julie Goodridge, HR Manager FOH, Tel. x2126, Email J.Goodridge@uea.ac.uk

Senior Resident Tutor

David Thurkettle, Senior Resident Tutor, DOS, Tel. x3730, Email D.Thurkettle@uea.ac.uk

INTO

Ruth Courridge, Head of Student Services, Tel. x1857, Email Ruth.Courridge@uea.ac.uk
Bob Parsons, Student Services Manager, Tel. x1048, Email Bob.Parsons@uea.ac.uk