Sample Managed Workstation Incident Response Workflow

1. Incident Report
   - Does the workstation have restricted data on it? [Yes/No]
2. If No, go to dispute.
3. If Yes, go to step 3.
4. Does the workstation connect to a system with restricted data? [Yes/No]
   - If No, go to dispute.
   - If Yes, go to step 4.
5. Does the workstation user log into applications with restricted data? [Yes/No]
   - If No, go to dispute.
   - If Yes, go to step 5.
6. Breach? [Yes/No]
   - If No, go to dispute.
   - If Yes, go to step 6.
7. Re-image Workstation
8. Replacement Workstation
9. Notify Unit Management and ISO / SIRT
10. Log Exception
11. "Clean" Workstation
12. Determine root cause
13. Adjust procedures
14. Close Incident

Exception