# Information Security and Continuity Management (ISCM)
# Frequently Asked Questions

1. For desktops/laptops, what is the process for installing software that is not part of the normal desktop software offerings?

   Any software not on the standard desktop image for ITS is considered Category 3 – Non-Standard Software. Category 3 software requires a documented business justification for use and management approval prior to installation. To initiate the process for installing non-standard software, submit a Remedy ticket to the ITS Service Desk and have it assigned to Desktop Services. Non-approved, non-business software such as games, tax software, password vaults, etc., will not be loaded on ITS-managed devices.

2. How can I be sure my software meets all the requirements of the North Carolina Statewide Security Standards (SWS) or other applicable governances?

   If you operate an application hosted on an ITS-managed device and you think the application might not meet all the NC SWS, a deviation may be required. Information Security and Continuity Management (ISCM) can perform a review of your situation to determine if a deviation is required. To request a security review, submit a Remedy ticket to the Service Desk requesting an ISCM review for compliance.

3. What is the process for requesting a deviation from NC Statewide Security Standards (SWS)?

   Download the deviation request form from the Enterprise Security and Risk Management Office (ESRMO) website at the following location: http://www.esrmo.scio.nc.gov/security/default.aspx. Fill out the deviation request form and submit it to your agency Security Liaison for review.

4. Why do I need a Business Continuity Plan (BCP)?

   Business continuity planning provides a quick and smooth restoration of operations after a disruptive event. Business continuity planning is a major component of risk management and includes business impact analysis, business continuity plan (BCP) development, testing, awareness, training, and maintenance. As state government agencies, we address business continuity planning because it's the law. The consequences of not planning may negatively impact the health and safety of the state's citizens, finances, operations and reputation.

5. How often should the BCP / DR (Disaster Recovery) plans be reviewed?

   Legal and regulatory requirements say at least annually. However, all agencies should closely monitor their critical business environments for changes and issue updates as needed.

6. What are some guidelines for identifying mission critical functions?

   Functions should be considered critical if any of the following apply:

   - Support primary mission statement
   - Support other agencies' mission critical function
   - Must be recovered quickly
   - Have a high dollar value
   - Have a high business impact
   - Have political ramifications or implications
   - Have legal requirements or liabilities

7. When I have questions regarding my BCP / DR plans, who at ITS should I contact?

   Depending on the task being questioned, there are several teams that may be involved. The first step is to contact the ITS Service Desk and open a Service Request ticket.  If necessary, the Business Relationship Management team member assigned to your agency will assist and coordinate activities in a real emergency.

8. How do I know if ITS is prepared to provide Disaster Recovery for my Distributed Hosted applications at the ITS Eastern Data Center (EDC)?

   Check your Service Level Agreement (SLA) with ITS. If there is no specific agreement for recovery with Recovery Time Objective (RTO) time frames, you should ask your Business Relationship Manager for verification.

9. How can I create a strong password that is also easy to remember?

   There are numerous ways to develop passwords that are easy to remember but still hard to crack. One method is to think of a phrase, rhyme, song, book passage, etc., that you know by heart. For the passage, use the first letter from each word as one of the letters of your password. For example “**T**he **q**uick **r**ed **f**ox **j**umps **o**ver **t**he **l**azy **b**rown **d**og” would be “TqrfjotlbD”. This is a good password; however, it does not contain any numbers or special characters. To make the password stronger, add a number and special character to the phrase. For example change the phrase to “**T**he **q**uick **r**ed **f**ox **j**umps **o**ver **2** **l**azy **b**rown **d**ogs**!**” The final password would read “Tqrfjo2lbD!” which is a strong random password that should be easy to remember.

10. What are things to avoid when creating a password?
    - Do not use the same password for both work and personal accounts.
    - Do not use dictionary words.
    - Do not use easy to guess personal information for passwords such as date of birth, anniversary date, family member names, pet names, etc.
    - Password vaults or software that is designed to store all of your passwords are not allowed per Statewide Security Standards.
    - Do not write your passwords down (even on a hidden sticky note).