Security Division ONE – New Hire Onboarding

Welcome to the NFCU Security Division. We're excited to have you on our team. You're joining a diverse group of team members all dedicated to a common goal — prepare, prevent, and protect our members and organization from fraud. Our members are the mission. As those who serve our members, you are our mission.

Onboarding at a new organization can be quite a busy time. This Onboarding Journey is automatically assigned to new team members and their leaders in the My HR System. This task list provides important information when it's needed, throughout your first week of employment.

As a new team member, you'll get a list of tasks that need to be completed including everything from reviewing the department handbook and becoming familiar with your job role responsibilities to understanding the Security Division's holistic operation. The system is intuitive enough to know what information is needed for your job role.

All components of the "Security ONE" are included in the specialization within Navy Federal University and should be completed within the first week of onboarding to the Security Division. Specific completion guidelines are included on individual components as applicable.

Note: It is important to follow the due dates in your journey to meet Navy Federal requirements and state laws, ensure that you are properly onboarded, and grow a successful career at Navy Federal!

REQUIRED PREREQUISITES: NFCU ONE - New Hire Onboarding ILT
All employees are required to complete this course prior to beginning the Security Onboarding program.

ESSENTIAL CONTACT INFORMATION

Supervisor Information	Office Hours
Supervisor Name: Work Email: Phone Number:	M-F 8:00am – 4:30CT / 9:00AM – 5:30ET

Note: Your immediate supervisor may provide you with additional essential contact information that is not listed in the department handbook found in module one of this course.

Security Trainer Contact	Office Hours
Trainer Name and Title: Work Email: Phone Number: WebEx:	M-F 8:00am – 4:30CT / 9:00AM – 5:30ET **Note:** Please reference Webex Status for availability.

Note: For any questions or concerns regarding this course or the Security Basic Training session please contact your assigned trainer by email or WebEx. All responses will be made within 48 hours of receipt during the listed normal office hours.

SECURITY ONE TRAINING COURSE INFORMATION

DESCRIPTION: The Security ONE training program is a blended new hire training program designed to familiarize new hires with the Security division and is the prerequisite course for all Security Division skill and technical training programs completed by new hire employees. The information in this course has been divided into modules designed as a checklist that will provide any resources needed to ensure employees complete all necessary new hire action steps and are provided with appropriate resources for their new job role to ensure a great start at Navy Federal. This course includes a module for the synchronous Security Basic Training Session that provides an overview of the Security Division.

COURSE OBJECTIVES:

Upon completion of this course, participants will be able to:

- Describe Who Navy Federal Is & Who We Serve
- Understand Navy Federal's Mission Statement and State Security's Mission
- Define Fraud and Distinguish the Different Types of Fraud
- Locate Security Organizational Charts
- Describe Fraud and Physical Security Divisions
- Recognize Differences Between All Branches of Fraud and Physical Security Division
- Identify and describe the responsibilities for all five branches within the Fraud Operations Department and the correlation to their job role.
- Recognize and articulate their job role's responsibilities within their department and the Security Division.
- Translate Your Role as It Applies to Security Organizational Goals, Fraud Strategy, and Mission
- Allocate Member Scenarios to the Appropriate Security Team/Workstream.

COURSE LENGTH:

Security ONE Onboarding Course: 15 Modules

- Security Basic Training Session: 1 Module - 6 hours
    - This session is scheduled by the assigned Security Trainer.
    - Training Time: Includes 1 hour lunch and two breaks.

EVALUATIONS:

- Knowledge check assessments
- Group discussion
- End of course Survey
- 60-Day Questionnaire (Post Training Interview)

REQUIRED COURSE RESOURCES:

The following resources will be provided to participants for course completion.

- The Security Division eNet Manual Pages
- The (***Department Title***) Onboarding Handbook
- The Basic Training Participants Guide
- Job Shadow Participants Guide Notebook

FACILITATION AND TRAINING STRATEGIES:

The methods of instruction for this course include lectures, videos, group discussions, individual and group activities, observations, mentor sessions, independent study, as well as knowledge checks.

FIELD ACTIVITIES:

This course is comprised of several different field activities that are required for course completion. Activities include participation in shadow sessions with an assigned mentor from your department as well as job shadow sessions with a SME from all five Fraud Operation branches.

COURSE COMPLETION:

Failure to complete an activity or module will result in an incomplete for the overall course. All modules must be satisfactorily finished for the course to be marked complete.

Course completion will be determined based on the following criteria:

- All knowledge check assessments completed with an 80% or higher.
  Note: Participants will be allowed an unlimited number of attempts to complete all assessments.
- Completion of the synchronous Security Basic Training Course.
  Note: Attendance and module will be marked complete by the Security Trainer.
- Attend all scheduled Meet and Greet sessions satisfactorily – verified by their direct leader and marked complete.
- Attend all scheduled shadow sessions (group or individual) verified and marked complete by Trainer.
  Note: The Assigned Trainer will assist participants with obtaining SMEs and scheduling shadow sessions for Fraud Ops.
- Satisfactorily complete all discussion and group activities reviewed by the Trainer/Facilitator.

SECURITY ONE: COURSE ELEMENT DESCRIPTIONS

The modules in this course contain the following components

DEPARTMENT HANDBOOK:

Participants will receive a copy of their departmental handbook, which outlines the policies, procedures, and job role expectations. This handbook will serve as a reference for completing all necessary new hire checklists and tasks. It is essential for all employees to be acquainted with the policies and procedures relevant to their respective departments as detailed in this handbook.

SECURITY BASIC TRAINING COURSE:

This is a six-hour synchronous training session that all participants are required to attend. This session provides new hire security employees with an overview of the Security division and how we prepare, prevent, and protect from fraud. Participants will engage in different discussions and activities to gain a thorough understanding of each department and their operations.

Note: The *Security Basic Training* course is a synchronous session that will be scheduled by the designated security trainer for all new hire employees. This course is typically trained at the start of any

new hire course; however, it can be facilitated as a stand-alone course. This module is required for course completion.

KNOWLEDGE CHECK ASSESSMENTS:

Participants will take a minimum of five knowledge check assessments (100 points each) during the course.

- Knowledge checks may show up as tests for specific weeks or lessons, or in a midterm or final assessment format.
- Graded assessment expectation for is generally 80%. While 80% is the expectation, learners are not prevented from completing training solely based on Knowledge Check scores.
- Trainers are expected to coach to the questions missed and offer additional assistance as needed to ensure the trainee's future understanding moves forward.

FRAUD OPS SHADOW SESSIONS:

There will be five job shadow sessions that will be scheduled based by the new hire employee's immediate supervisor. New hires will observe a tenured Investigator/SME from each of the five Fraud Operations branches perform job duties. Investigators from each branch will provide an in-depth overview of job responsibilities and systems used for fraud mitigation. Participants will complete a DBLA post on the Security Training community board for each shadow session.

DISCUSSION BASED LEARNING ACTIVITY (DBLA):

There will be a total of five DBLA posts that you will be required to complete. These activities will assist you with reflecting on each job shadow experience and how your prospective job role and responsibilities correlate with the different Fraud Operations branches to mitigate fraudulent activity to serve the Security Division's mission.

TECHNOLOGY REQUIREMENTS

This course requires regular access to your company-issued laptop as well as a stable internet connection when working remotely. Participants are responsible for acquiring and maintaining regular access to the company-issued headset with a microphone and a webcam. The use of a webcam and a headset with a microphone is essential for active participation in course activities. These tools will enhance interactivity within the course and facilitate communication with both the instructor and fellow participants.

Note: Please ensure you have reviewed the organization's policy for internet service provided requirements to avoid outages and attendance incidents which may result in disciplinary actions.

Computer Specifications:

The company issued laptop specifications may vary based on job role. Participants will be issued a laptop by ISD at their immediate supervisor's request prior to the start of this course. Please direct any questions regarding laptop specifications to your immediate supervisor.

Note: While mobile devices can be used to access WebEx applications to attend scheduled synchronous sessions or check and respond to messages, participants are required to attend all security training sessions via their laptop. Failure to do so may result in disciplinary action up to termination.

SECURITY TRAINING EXPECTATIONS AND POLICIES

Employees participating in Security Training classes are expected to adhere to the Security Training Expectations and policies outlined below.

COMMUNICATION EXPECTATIONS:

Security Training classes are considered a professional environment where discussions and learning take place. Participants are expected to make every effort to maintain this environment as a safe place for everyone to share opinions, ideas, ask questions, and collaborate professionally.

- Choose your words **carefully**. When communicating through WebEx, words or messages could be misunderstood. Proofread messages to consider how others may interpret them.
- Keep an open mind to other perspectives. Be polite and respectful to opposing opinions.
- Use correct spelling, grammar, capitalization, and punctuation in all correspondences. Use standard English, not "texting" abbreviations or shorthand.
- Do not use CAPS lock as this indicates anger, aggression, or can be perceived as demeaning.
- Be **culturally** sensitive. NFCU proudly promotes Diversity and Inclusion. Be careful with humor or jokes as well as context to avoid offending others.
- Be open to constructive criticism and feedback from others.
- Respect other people's time. Written communication via messengers can take time to write and read. Online communication should be direct and to the point when applicable.

PARTICIPATION EXPECTATIONS:

Participants should be active in class. To fully engage in the learning process everyone is encouraged to participate in all course activities and to be proactive about asking questions.

- Use the hand raise tool, WebEx meeting or the WebEx class chat when asking questions.
- Be patient when waiting for written responses. It may take time for others to type a response.
- Keep mics muted unless contributing to discussion or asking questions to prevent distractions.
- Be prepared to share work when requested during synchronous sessions.
  Note: Trainers may call on learners to contribute or participate in various activities or discussions.

WEB CAM EXPECTATIONS:

Participants are expected to have their webcams turned on during all synchronous sessions unless directed otherwise by their instructor.

TRAINEE CONCERNS REGARDING COURSE AND/OR MATERIAL:

If you believe that the course objectives are not being met, or that you are finding it difficult to keep up with the pace of the course, we ask that you:

- Bring the issue to the attention of the trainer within the same day, preferably during the lesson be facilitated if comfortable.
- Discuss and agree upon a remediation plan with the trainer that will address the issue whilst continuing with the course attendance.
- If you do not feel comfortable addressing concerns with your trainer, you are expected to communicate concerns to your immediate supervisor.

If you believe you are attending the wrong course, or do not meet the pre-requisites we ask that you:

- Notify the trainer immediately so that remedial actions can be discussed and taken.

POWER AND INTERNET OUTAGES:

Training classes held online in a virtual environment has a unique set of challenges such as power/internet outages due to equipment malfunctions. Learners are expected to communicate technical issues that result in their absence from class for any extended period of time (five or more minutes). Uncommunicated issues may contribute to the documentation of attendance instances.

- Trainers will set expectations with learners at the start of class regarding communication during outages or tech issues. As a rule of thumb, any outage lasting more than a couple of minutes should be communicated with a trainer so the trainer knows the learner's status and may provide next steps for troubleshooting.
- Employees should follow the guidance found on the Telework Outage Resource page for power or internet outage procedures.
- The proper procedures for timekeeping during outages may be found within the Teleworker Timekeeping SOP and should be followed for reporting.
- Any questions that cannot be answered utilizing the included resources may be directed to the immediate Supervisor.

GENERAL TECHNICAL ISSUES:

Security trainers are adept and maintain strong technical skills with organizational systems. Trainers can troubleshoot any technical issues that occur.

The following are general expectations participants should follow when experiencing technical problems:

- Notify the trainer of the technical issue immediately through appropriate communication channels.
- If applicable send screen shots to assist Trainer with identifying and troubleshooting issues.
- Be prepared to share your screen to assist the Trainer with troubleshooting procedures.
- If a reboot/restart is needed, participants are expected to log back in promptly.
- Do not call HD or submit any Somethings Broken or MyIt tickets unless directed by the Trainer.

Participants experiencing technical issues that prevent or interrupt participation or attendance to virtual classes are expected to communicate issues experienced to their trainer or immediate supervisor promptly.

- Participants who are late to virtual classes due to technical issues that were communicated with Trainers via WebEx Teams chat will not be considered tardy.
  - The Trainer will **not** send a tardiness email regarding timeliness.
  - The arrival time to class will be tracked with explanation and supported documentation such as an email from Help Desk.
  - Three late arrivals due to technical issues is considered a trend. Trainers will report via email to the appropriate parties to address and help the participant find solutions.
- Participants who are late due to technical issues that **were not** communicated before the start of class through WebEx teams will not be considered tardy. However, Trainers will advise of communication expectations with the participants as well as notify direct supervisors.

ATTENDANCE POLICIES

Regular and predictable attendance is a mandatory job requirement for all new hires. Security Division employees are required to adhere to the Training Department's established schedule of 8 hour and 30-minute days, with a 30-minute unpaid meal and two 15-minute paid breaks.

ATTENDANCE POLICY:

- All new hires are expected to attend all onboarding classes to which they are assigned without absences.
- Absences during the onboarding probation period may result in disciplinary actions to include termination.
    - Exceptions to the attendance policy may be made on a case-by-case basis. Leadership will consider the length of class, content missed, participant performance, and nature of absence, department policies and training capacity if deciding whether to re-class the participant or make exceptions to the attendance policy.
- Participants are expected to arrive on time and to return on time from all lunches and scheduled breaks.
    - **On-time in virtual classes** means that the participant is present within the session, dialed into the session, and responds when prompted to indicate that they are listening. Participants will be given a 5-minute grace period in the morning to log in before Trainers send an email communication to immediate supervisors regarding attendance.
    - **On-time in live classes** means that the participant is seated with their computer active and attentive to the Trainer.
    - Trainers must clearly communicate a return time for any additional or extended breaks.
    - Trainers ***may*** increase break time granted to participants at their discretion if needed, however:
        - Participants should never be given less than 30 minutes of meal and 30 minutes of break.
        - Participant timesheets should always reflect a 30-minute unpaid break.
        - Trainers must be mindful of the scope and sequence to plan breaks appropriately to ensure content is delivered in accordance with the class schedule.

LATE ARRIVALS AND EARLY DEPARTURES:

In addition to absences, late arrivals, and early departures, it may be considered an attendance trend if participants are deviating from the break schedule without trainer approval. Attendance trends of any type will be documented and discussed with the participant to reinforce expectations.

- For tardiness exceeding 2 incidents, Trainers will communicate with direct leadership regarding occurrences and disciplinary actions.

SEFCURITY TRAINING CODE OF CONDUCT

All employees are expected to abide by the NFCU Code of Conduct. Participating in virtual and/or hybrid training might be different from previous experiences you may have had. Given that the elements of this course take place in a variety of settings, participants are expected to follow the guidelines outlined below to ensure everyone can benefit from a positive learning experience.

Demonstrate respect and consideration for all people.

- Avoid dominating the microphone or airtime. In a virtual meeting, mute audio when not speaking.

- Participation always requires responsible behavior from you together with respect towards other participants and coworkers. NFCU follows a zero-tolerance policy and treats all forms of abuse, bullying, intimidation, sexist and racist behavior very seriously.

Communicate openly and thoughtfully with others, listen well to others, and be considerate of the multitude of views and opinions that are different than your own.

- Make room for a diversity of voices in group discussions, questions, or chats.
- Facilitators will invite discussion but are sensitive not to pressure those who have not communicated to do so.

Be respectful when discussing and debating ideas.

- Demonstrate that differing perspectives are valued—critique ideas, not people.

Be collaborative.

- Be mindful not to exert dominance over others.
- Be tentative to imbalances in relationships, roles, and experiences, as well as the advantages of video communication over audio or other methods, in order to mitigate the risk of dominance.

Be mindful of your surroundings and of your fellow participants during an in-person event.

- Please be aware of your surroundings, particularly if your online activity enables you to share your video or microphone. Ensure that your backdrop is appropriate for a classroom setting, and if there are any unexpected noises etc. (including noisy family members!) please mute your microphone or stop the video as needed, until you are safely able to re-activate.
- Do not take photographs of your screens or share any images of the online session, this is for your safety as well as the safety of other learners, co-workers, and the organization.

Report concerns your trainer or supervisor so that they can be addressed responsibly and in a timely fashion.

- If you are reporting a concern regarding another participant, respect the identity of any individual(s) involved by maintaining confidentiality.
- If you are questioned as part of an investigation or review of a conduct concern, answer questions in a forthright and complete manner.

If a Trainer or any Leader directs you to stop a behavior or delete a comment, comply immediately.

- Such directions are made to implement this policy or the organization's policies.
- If your behavior is inappropriate in any way, Trainers are authorized to immediately mute the microphone/stop video/stop chat access as needed and warn you that if the behavior continues, you will be removed from the training session.
- If the behavior is serious enough it could lead to disciplinary actions including termination.