COASTAL
COMMUNITY BANK

EMPLOYEE HANDBOOK

Approved by BOD
December 14, 2022

Table of Contents

This handbook is designed to acquaint you with CCB, hereinafter referred to as "CCB" or "Bank" and provide you with information about working conditions, employee benefits, and some of the policies affecting your employment. You should read, understand, and comply with all provisions of the handbook. It describes many of your responsibilities as an employee and outlines the programs developed by CCB to benefit employees. One of our objectives is to provide a work environment that is conducive to both personal and professional growth.

No employee handbook can anticipate every circumstance or question about policy. As CCB continues to grow, the need may arise and CCB reserves the right to revise, supplement, rescind, interpret, apply, or depart from any policies or portion of the handbook from time to time as it deems appropriate, in its sole and absolute discretion. Employees will be notified of written changes to the handbook as they occur. Information in company manuals, employee handbooks, employment applications, company memorandums, or other materials provided to employees in connection with their employment, should not be construed as a promise of specific treatment in specific situations, of permanent employment, of employment for any particular length of time, of discharge only for cause, or of a right to any particular corrective action or discharge procedures.

MISSION STATEMENT

CCB's mission is to provide financial services to help small business owners, and other community minded individuals who see the value in partnering with a local bank. Our employees utilize their strengths to set the course and are empowered to do the right things for their clients.

WHY WE'RE HERE

No other bank knows better than we do what it takes to thrive as a small business. And for CCB, an organization that aspires to maximize our potential to help our client's business, our mission is a given. To realize our mission, we must stay true to a set of core values. These values aren't negotiable. They don't change. They define who we are and what we stand for.

1) **Stay Flexible** – We realize things change-and when they do, we need a plan B, C, and D.
2) **Take Care of Each Other** – If we have stronger teams, we're going to win more often.
3) **Embrace Gray Thinking** – We like people who are able to function in a fluid environment.
4) **Be Relentless** – We don't stop until we've exhausted every last resource.
5) **Be the Best** – We look for people who have the talent and skills to outwork our competition.
6) **Be Un-Bankey** – We strive to let go of tradition and standard modes of operation in our industry.

When it comes to making a positive difference in our communities, we are equally committed to helping find a way. Our voluntary Employee Giving Program is a testament to our commitment to be an integral part of the communities where we live and work. Every employee's contribution is valued, whether it be supporting the employee giving fund, volunteering in their community, or serving on a board. Helping our neighbors is at our core.

The integrity of our employees is of the highest importance to CCB Community Bank. Should you ever feel you are being asked to do anything you feel is fraudulent or inappropriate please bring it to the attention of Executive or Senior Management. If you are not comfortable going to anyone on the Executive or Senior Management team, you may contact Human Resources or the Chairman of the Audit Committee or contact **www.lighthouse-services.com/coastalbank** or 833-222-3893 for reporting purposes.

EQUAL EMPLOYMENT OPPORTUNITY

It is the policy of CCB to provide equal opportunity for all qualified persons and to strictly prohibit discrimination against any employee or applicant for employment because of race, color, religion, gender, sexual orientation, gender identity, age, national origin, marital status, military status, disability, genetic information or any other protected status. It is the intention of CCB to act in accordance with all regulations of the federal, state, and local government in respect to providing equality of opportunity in employment.

CCB is committed to employing only United States citizens and aliens who are authorized to work in the United States and does not unlawfully discriminate based on citizenship or national origin.

All Employment Posters are located on each premises and on the intranet Human Resources page.

CUSTOMER SERVICE STANDARDS

CCB is committed to giving our customers the best possible service. At CCB it is our policy that although the customer is not always right, they are *always the customer*.

Stop and reflect on how you like to be treated when you are a customer. It is easy to envision what good customer service looks like. Our aim is to make our customers feel that they are honored guests. Greet the customer, listen to their questions, and thank them for allowing us to assist them with their needs.

Our high standard of customer service extends beyond what we might think of as external customers. This superior level of courtesy should be maintained in all contacts with clients, customers, co-workers and any and all persons you come in contact with during the business day.

HUMAN RESOURCES RECORDS

It is important that Human Resources files be kept current. This ensures, among other things, that benefits are properly administered. To keep files current, employees are asked to update their employee profile in our online Human Resources portal immediately of any changes to the following:

- Name
- Address and/or telephone number
- Marital status
- Dependents
- Designated beneficiaries
- Emergency contact

With reasonable advance notice, and as required by applicable law, employees may review their own HR files virtually or in CCB's offices and in the presence or virtual observation of an individual appointed by CCB.

EMPLOYEE RELATIONS

CCB believes that the work conditions, wages, and benefits it offers to its employees are competitive with those offered by other employers in this area and in this industry. If employees have concerns about work conditions or compensation, they are strongly encouraged to voice these concerns openly and directly to their managers.

Our experience has shown that when employees deal openly and directly with supervisors, the work environment can be excellent, communications can be clear, and attitudes can be positive. We believe that CCB amply demonstrates its commitment to employees by responding effectively to employee concerns.

ANTI-DISCRIMINATION/ANTI-HARASSMENT POLICY

At CCB we believe that employees should and must treat one another with dignity and respect. CCB does not discriminate on the basis of race, color, religion, gender, sexual orientation, gender identity, age, national origin, marital status, military status, disability, genetic information, or any other protected status. Employees of CCB must respect and uphold this policy. Harassment of any kind will not be tolerated, including slurs or jokes based on any of the above categories. Anyone violating this policy will be subject to disciplinary action up to and including termination.

Illegal workplace harassment is a form of employment discrimination that is prohibited by federal, state, and local laws. To be harassment, the conduct or words must be (1) unwelcome or unwanted; (2) directed against someone because of their "protected class status" (their race, sex, religion, national origin, disability, and other specific bases set out in each law) and (3) sufficiently frequent or severe as to cause the reasonable person to find their workplace offensive, hostile or intimidating. At CCB we aim to cultivate a workplace that is productive and free from any conduct that may be deemed as harassment.

Sexual Harassment

CCB will not tolerate sexual harassment of any kind. This standard applies to all employees, vendors, clients, customers, and guests. Any instance of sexual harassment will be vigorously investigated. Any employee found to be engaging in any form of sexual harassment will be subject to severe disciplinary action up to and including termination. Any non-employees engaging in sexual harassment on company property or at company events will also be subject to severe corrective action. Employees should be aware that civil penalties that can be imposed for violating the laws against sexual harassment. Sexual harassment is one type of workplace harassment.

What is Sexual Harassment? The Legal Definition:

On September 23, 1980, the Federal Equal Employment Opportunity Commission adopted the final guidelines on sexual harassment. Harassment on the basis of sex is a violation of Sec. 703 of Title VII of the Civil Rights Act of 1964 (#1604.11). Under Title VII, unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute harassment when:

- Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment.
- Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual.
- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.
- Includes sexual displays of consenting parties that create an intimidating, hostile or offensive working environment that offend a third party.

In lay terms, sexual harassment is: unwelcome or unwanted sexual advances, suggestions, requests or demands for sexual favors, or unfavorable treatment upon aversion to such requests, verbal abuse, printed material, emails, gestures or jokes that are sexually oriented and considered tasteless or unacceptable by another, interfering with a co-worker's performance by offering unwanted sexual

attention or sexually oriented conduct that reduces personal productivity creating or permitting an intimidating, hostile or offensive work environment.

Complaint Procedure

If you believe you have been or are being harassed, you should take the following steps:

- Contact Human Resources, concerns or complaints will be promptly investigated and upon findings of wrongdoing, immediate disciplinary action will be taken. It is important to report any conduct that continues to bother you, even if you're not sure it is illegal harassment
- Confidentiality of both complainant and accused harasser will be maintained if at all possible. Though every effort will be made to uphold confidentiality, it is sometimes necessary to disclose details of a circumstance or complaint to effectively investigate and take appropriate action. Disclosure of information gathered during the investigation will be restricted to those with an absolute "need to know"
- Under no circumstance will employees suffer retaliation for reporting such concerns or for cooperating with any investigation. CCB will not tolerate retaliation of any kind. Any retaliatory behavior will be met with swift and severe corrective action up to and including termination

CCB views the business ethics of its employees as an important matter. An employee, who has doubt as to whether or not he/she is in compliance with this Policy, has an obligation to refer the matter to Executive management for a decision, and if unresolved, to Michael Patterson, Chairman of the Audit committee for the Board of Directors. Mr. Patterson can be reached at mpattemail@gmail.com. Disciplinary action, up to and including discharge, will be taken against:

- An employee who authorizes or participates in an action or omission that violates this Policy or the law or who knowingly falsely accuses another employee of such a violation.
- A supervisor or manager who endorses or who fails to prevent or report a violation of this Policy or the law or who retaliates, or condones retaliation by others, against an employee who reports such a violation.

In determining whether and if any, the type of discipline to be imposed, CCB may take into consideration factors which include, but are not limited to, the degree of participation in and/or knowledge of the violation, whether the conduct could otherwise be explained or justified, and the type of violation and/or consequences.

Unlawful Harassment Defined

Unlawful harassment is defined as verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of his/her protected class status, or that of his/her relatives, friends or associates; and that (1) has the purpose or effect of creating an intimidating, hostile or offensive work environment; (2) has the purpose or effect of unreasonably interfering with an individual's work performance; or (3) otherwise adversely affects an individual's employment opportunities.

Unlawful harassment can take many forms and can include, but is not limited to:

- Jokes, comments, innuendo, or other remarks that are "off color" or derogatory to a person based on his or her sex, race, color, national origin, age, religion, creed, real or perceived sensory, mental or physical disability, sexual orientation and gender identity and expression, genetic information, marital status, honorably discharged veteran or military status, or any other characteristic protected by applicable federal, state or local law
- Pictures, cartoons, articles, or centerfolds that are sexist or derogatory as listed above
- Unwanted, inappropriate, or offensive looks, touches, gestures, or other physical conduct

PERSONAL RELATIONSHIPS IN THE WORKPLACE

The employment of relatives or individuals involved in a dating relationship in the same area of an organization may cause serious conflicts and problems. For purposes of this policy, a relative is any person who is related by blood or marriage. Dating, romance, or fraternization (hereinafter referred to as a "dating relationship") is defined as a relationship of an intimate or close personal nature including dating, engagement, or cohabitation.

Employment of relatives or individuals in a dating relationship with a current employee is not allowed under circumstances that, in the sole discretion and judgment of CCB, pose problems with respect to a manager/subordinate relationship, security or a possible conflict of interest. In particular, CCB does not permit employment of relatives or individuals in a dating relationship with a current employee when one employee will be responsible for auditing, supervising, or reviewing the work or performance of his or her relative or of an individual in a dating relationship with him or her. If a relative relationship or dating relationship is established after employment begins between employees who are in a reporting or other "conflict of interest" situation as described above, it is the responsibility and obligation of the supervisor or more senior employee involved in the relationship to disclose the existence of the relationship to management. The individuals concerned will be given the opportunity to decide who is to be transferred to another position, if one is available. If that decision is not made within 30 calendar days, management will decide, in its sole and absolute discretion, which is to be transferred or, if necessary, terminated from employment.

JOB POSTING

At CCB we believe in promoting from within whenever possible, and we support and encourage each employee to realize his or her full potential. Opportunities to advance will be based on proven skills and ability, achieved results, and performance records. An internal job application must be completed and approved before being considered an applicant.

While current employees are given consideration for job openings, this may not always mean that they will be placed ahead of outside applicants. Our goal is to place the best-qualified candidate in each position.

Hiring Referral Bonus

CCB offers a referral bonus to employees upon hire of a referral. The referring employee's name must be on the new hire's employment application in order to qualify. Temporary employees and intern referrals are not eligible for a hiring bonus. Managers are not eligible for referrals that report to them.

FIDELITY BOND

Every employee of CCB is responsible for all monies, funds, valuables, and/or property, which may be placed in his or her hand or possession as an employee of CCB. All employees shall be bonded at the expense of CCB, either in one or more blanket bonds, or in separate bonds. The amount and form of bonding will be determined or adjusted from time to time as determined by the Board of Directors. Any employee who cannot be appropriately bonded will be subject to disciplinary action, up to and including immediate termination.

FIRE, ROBBERY AND OTHER EMERGENCIES

In the case of an emergency that threatens the operation of the office or endangers life or property, the most important thing to do is to remain calm. If you see a potentially serious occurrence, do the following:

- Call 911
- Give your name, the name and address of your location, and the nature and location of the emergency within the office
- Report the emergency to your manager
- Help move customers, guests, and other employees away from the danger area. All employees should be familiar with posted evacuation routes
- If total evacuation is necessary, an Evacuation Coordinator should remain in the department until the area is clear and then exit the building
- Be aware of the latest posted emergency preparedness information

Even small fires should be reported immediately to 911. Fire extinguishers are visibly located in our building and should be used.

Robberies
A “security officer”' has been delegated the responsibility and authority to ensure that all personnel are familiar with CCB's procedures and conduct in the event a robbery does occur. Refer to your branch “Robbery Kit” box for instructions on what to do. It is important that, if a robbery occurs, this situation be handled in such a manner as to protect bank customers and employees from danger and also to accumulate as much information as possible to aid in the apprehension of the criminal.

Violent or Disruptive Behavior
If you see anyone acting in a threatening manner or disrupting the business, you should call your manager or Human Resources immediately. Do not confront the individual(s) in a way that might make them even more disruptive. Call 911 if appropriate.

Threatening Phone Calls
If you ever receive a threatening telephone call, whether the threat is directed at you, a co-worker, or the company, you should turn the call over to a manager.

INCLEMENT WEATHER

Unless the office is closed for the day, all time missed will be charged to vacation or, if none is available, then to unpaid time off.

EMPLOYMENT STATUS AND RECORDS

It is the intent of CCB to clarify the definitions of employment classifications so that employees understand their employment status and benefit eligibility. Each employee will belong to one of the categories listed below.

FULL-TIME SALARY employees are exempt employees. They are eligible for CCB's benefit package, subject to the terms, conditions, and limitations of each benefit program. Exempt employees are excluded from specific provisions of applicable federal and state wage and hour laws. An exempt employee does not receive overtime for hours worked over forty per work week.

FULL TIME HOURLY employees are non-exempt and work between 30 and 40 hours per week. They are eligible for CCB's benefit package, subject to the terms, conditions, and limitations of each benefit program. Non-exempt employees are entitled to overtime pay at a rate of one and one-half the times (1 ½) of their regular pay for hours worked more than forty (40) hours in a workweek.

PART-TIME HOURLY employees are non-exempt employees. They are regularly scheduled to work less than a full-time hourly work schedule, but at least 20 hours per week. They are eligible for CCB's benefit package, subject to the terms, conditions, and limitations of each benefit program. Non-exempt employees are entitled to overtime pay at a rate of 1 ½ times their regular pay for hours worked more than forty (40) hours in a workweek.

ON CALL/VARIABLE employees are non-exempt. They do not have regularly scheduled hours and work on an on-call basis. While they do receive all legally mandated benefits and are eligible to enroll in the 401(k) plan if they are at least 18 years old, they are ineligible for all other CCB benefit programs.

INTERNS ON SCHOOL BREAK are non-exempt employees. They are students on break from school and are hired for a pre-determined project or time frame. While they do receive all legally mandated benefits, they are ineligible for all other CCB benefit programs.

EMPLOYEE BENEFIT PROGRAMS

Eligibility for benefits begins on the first of the month. If an employee chooses to enroll at a date later than the first eligibility date, she/he may be subject to health exams and questionnaires prior to gaining approval for benefits.

Employees may or may not also be subject to waiting periods for certain health conditions if enrollment is delayed beyond the first eligibility date. If an employee chooses to cover dependents, they must be enrolled at the time of employee enrollment, within 30 days of marriage, birth, or adoption, or at the open enrollment date. Enrolling dependents later than their eligibility date may also result in a requirement for health exams and/or questionnaires.

Medical, Dental, and Vision Insurance

CCB's health insurance plan provides eligible employees and their dependents access to medical, dental, and vision benefits. Several plans are available to choose from. Spouses and dependent children may be added to the plan at the expense of the employee.

Life & Dismemberment (AD&D) Insurance

CCB offers a Paid Group Term Life Policy and Voluntary Life and AD&D insurance plans. Coverage is available to all full and part-time employees. See plan documents and enrollment for coverage details.

Long Term Disability Insurance

CCB provides a long-term disability (LTD) benefits plan to help eligible employees cope with an illness or injury that results in a long-term absence from employment. LTD is designed to ensure a continuing income for employees who are disabled and unable to work.

Vacation Benefits

Vacation time off with pay is available to eligible employees to provide opportunities for rest, relaxation, and personal pursuits or for other uses as allowed by law. Full and part-time employees are eligible to earn and use vacation time as described in this policy:

The amount of paid vacation time employees receive each year increases with the length of their employment as shown in the following schedule:

0 thru 3 years of Service	2 weeks
4 years through 6 years of Service or Assistant Vice President (AVP) title	3 weeks
7 years through 9 years of Service or Vice President (VP) title	4 weeks
Over 10 years of Service or Senior Vice President (SVP) title	5 weeks

Employees will receive ½ a year credit for each year of prior experience when they begin at Coastal. Example: If you have 10 years prior experience in a similar role as being hired for with Coastal, you will be granted 5 years credit towards the vacation accrual tier.

Eligible employees begin to accrue vacation the first of the month following date of hire. They earn paid vacation time according to the schedule and based on date of hire. You may take vacation time before it is earned, up to the amount you will accrue as of December 31st of that year. Your vacation accrual ceases during any unpaid portion of a leave of absence. Vacation time must be used during the year it is earned. Unused vacation time does not carry over to the next "benefit year" (applicable State and Provincial employment laws may apply.)

Paid vacation time can be used in minimum increments of one-hour by non-exempt employees. Exempt employees must take vacation days in 8-hour increments. Employees identified as being in a sensitive position will be required to take 5 consecutive workdays per year. See the Time Away from Office Policy on the Intranet.

Vacation is scheduled by seniority within department or branch with seniority based on date of hire.

Vacation time off is paid at the employee's base rate at the time of vacation. It does not include overtime or any special forms of compensation such as incentives, commissions, bonuses, or shift differentials.

If a paid holiday occurs during your scheduled vacation, the hours for that day will be recorded as holiday pay. If you become sick while on vacation, time off will be recorded as vacation and will not be converted to sick days. Paid vacation time must be exhausted before any requests for time off without pay will be considered.

Upon termination of employment, employees will be paid for unused vacation time that has been earned but not used through the last day of work. If employment is terminated mid-year, taken vacation that was not yet earned will be clawed back from final paycheck (applicable State and Provincial employment laws may apply.) If CCB, in its sole discretion, terminates employment for cause, forfeiture of unused vacation time may result.

Sick Benefits

CCB provides paid sick benefits to all eligible employees to care for their health and the health of their family members.

Benefits for Non-Exempt Employees

Non-exempt employees will accrue sick benefits at the rate of two (2) hours for every 40 hours worked. Sick benefits begin accruing on the first day of employment. There is no cap on the number of paid sick hours that may be accrued in a year for non-exempt employees. All eligible employees may access their accruals on the first of the month immediately following their date of hire.

Benefits for Exempt Employees

Exempt employees will accrue sick at the rate of 8 hours per month. Accrual commences at time of

employment and may be used as of the first of the month following employment. Exempt employees may carryover unused accrued sick hours into the following year; however, when unused accruals total 520 hours, further accruals will cease until the balance is less than 520. Exempt employees may use paid sick in increments of one day.

Employees will be notified of their accrued paid sick balances in the electronic payroll system which employee may access daily, including:

- Accrued sick balance since the last notification
- Used sick since the last notification
- Current balance of sick available for use

Because CCB must notify non-exempt employees of their usage and balance, it is the responsibility of employees to notify the CCB at the time of their absence that it is being taken for the purposes allowed for paid sick as described above.

Sick benefits will be calculated based on the employee's normal hourly compensation at the time of absence and will not include any special forms of compensation. Non-exempt employees may use paid sick in increments of 15 minutes.

CCB uses a calendar year for sick accrual, which means paid sick accrues from January 1 through December 31. Employees may carryover all hours of unused accrued sick into the following calendar year with no cap on maximum accrual. Sick accrual ceases whenever an employee is not working, whether paid or unpaid.

For absences of more than three (3) consecutive days, CCB reserves the right to require certification from a healthcare provider to substantiate the need and eligibility of paid sick time. The direct manager must also be contacted on each additional day of absence provided that this requirement does not interfere with the employee's use of sick time. Before returning to work from a sick absence for the employee's own health condition of five (5) calendar days or more, an employee may be required to submit a health care provider's verification that he or she is fit to return to work.
Unused sick benefits will not be paid out to employees while they are employed or upon termination of employment. When there is a separation from employment and the employee is rehired within twelve (12) months of separation, previously accrued unused paid sick shall be reinstated.

Wellness Days
CCB supports and is committed to the overall health and wellness, as well as improving the work-life balance of its employees. In order to provide a healthy work environment, CCB gives employees 2 Wellness Days per calendar year (16 hours). Mid-year newly hired employees will receive 1 Wellness Day. Wellness days are time-off for employees to focus on personal well-being and can be used for a variety of activities related to well-being. CCB believes that wellness days can have a positive personal and professional impact and allows employees to recharge so they can bring their happiest and most productive selves to work.

BENEFITS CONTINUATION (COBRA)

The federal Consolidated Omnibus Budget Reconciliation Act (COBRA) gives employees and their qualified beneficiaries the opportunity to continue health insurance coverage under CCB's health plan when a "qualifying event" would normally result in the loss of eligibility. Some common qualifying events are resignation, termination of employment, or death of a covered employee; a reduction in a covered employee's hours or a leave of absence; a covered employee's divorce or legal separation; and a

dependent child no longer meeting eligibility requirements under the terms of the applicable plan.

Under COBRA, the employee or beneficiary pays the full cost of coverage at CCB's group rates plus an administration fee as permitted by law. CCB provides each eligible employee with a written notice describing rights granted under COBRA when the employee becomes eligible for coverage under CCB's health insurance plan. The notice contains important information about the employee's rights and obligations.

EMPLOYEE PERKS

The following CCB perks are complimentary while you are an active employee, once no longer employed, all fees and charges will commence:

- Monthly service charge waived for one (1) personal checking account per employee
- Monthly service charge waived for one (1) personal savings account per employee
- Monthly service charge waived for one (1) IRA Account per employee
- No fee charged on Money Orders
- No fee charged on Cashier's Checks
- No charge for printed checks on one (1) personal checking
- Reduced Rate and No Annual Fee on Overdraft Protection Line of Credit
- No charge on one (1) Safe Deposit Box, smallest size only

Employees are not allowed to open, maintain, or process transactions on any account that they are a signer on, POD, or in any way an owner of.

Deposit Account Perks
Employee Money Market accounts will be eligible for a rate bump, at a rate of 0.15% basis points over regularly published advertised deposit rates. The Deposit Committees set rates are non-negotiable and are subject to change at any time.

To maintain the spirit of providing an employee perk during periods of competitive market rate increases, further rate bumps can be approved by any two of the following Senior Executives: CEO, President, CFO, or CBO/CLO. These would apply to all tiered pricing levels with no bumps or increases allowed to any individual employee account.

Employees will be eligible for the rate bump under the following requirements:

- Eligible on (1) one personal Money Market account. Employees may have multiple accounts, but only one would be eligible for the rate bump and it must meet all the following requirements:
    - Must be a personal Money Market account, not used for business or commercial purposes; and
    - Employee must be the main signer and account holder on the account receiving the rate bump; and
    - The account will be coded under the confidential employee account cost center
    - Employee must designate which (1) account they want the bump on.

If employment ends with Coastal, the rate will adjust to a published advertised non-employee rate in 30 days.

To request and designate which account you want for this special Money Market Account Rate bump, please complete an Account Maintenance form and submit to operations@coastalbank.com.

Loan Perks

Loans approved for employees shall be without CCB loan origination and processing fees. All third-party charges or out of pocket expenses will be paid by the employee. The employee rate will be at 1.0% below our normal posted rate at the time of application or at the time the rate is set on all CCB term loans.

CCB will decrease the margin by 1.0% on all Home Equity Lines of Credit. The Rate ceiling will be the same as our posted rate and the rate floor will be 1 basis point lower than our posted rate. CCB will decrease the margin by 1.0% on our Unsecured Personal Lines of Credit (grandfathered account). The Unsecured Personal Line of Credit does not have a floor – the rate ceiling will be the same as our posted rate. The Overdraft Protection account rate will be at 1.0% below our normal posted rate. Annual fees for each of the three accounts referenced above will be waived – all other third-party charges or out of pocket expenses will be paid by the employee.

Automatic monthly payments from a CCB employee checking account are available, but not mandatory. Employees will not be eligible for an additional .25% reduction in rate or margin for automatic payments on any CCB loan product.

Loans to officers may be subject to state or federal laws limiting the amount, requiring specific board approvals and/or limiting the availability of fee or rate discounts. We offer special pricing as referenced in paragraph 1 for our portfolio mortgages. Bank employees will receive a discounted fee (1/2 of our customary fee at the current rate) for every mortgage loan placed in the secondary market.

HOLIDAYS

Full-time employees will be eligible for eight hours of holiday pay for each qualified holiday. Eligible part-time employees will be eligible for four hours of holiday pay or equivalent to their normal work hours for the particular Holiday. Employees on unpaid leaves of absence will not be eligible for holiday pay.

CCB observes the following holidays and all offices will be closed:

- New Year's Day
- Martin Luther King Jr. Day
- President’s Day*
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veterans' Day
- Thanksgiving
- Christmas

*CCB conducts a mandatory paid all-staff meeting on the Presidents Day Holiday. All employees that attend the mandatory meeting receive an additional floating day off in lieu of the Holiday. Employees who do not attend the meeting will receive Holiday pay, if eligible, and will not receive an additional floating day.

CCB will grant paid holiday time off to all eligible employees immediately upon assignment to an eligible employment classification. Holiday pay will be calculated based on the employee's straight-time pay rate as of the date of the holiday.

If one or more of the federal holidays listed above should fall on a Saturday, employees will receive an additional day off in lieu of bank closure. You must have been employed with CCB at the time of the Holiday to receive this additional day. These days must be used within the calendar year they occurred. When a designated legal holiday falls on a Sunday, CCB will be closed on the following Monday, and no additional holiday provided.

VOLUNTEER TIME OFF POLICY

While most volunteer commitments take place after regular business hours. Some may require time off during the workday. To accommodate these situations, CCB provides all employees (full-time and part-time) with Volunteer Service Paid Time Off (VTO). Full-time employees may take up to 16 hours of paid time off each year to participate in their specific volunteer program(s). Part-time employees are eligible for 8 hours per year. Hours can be taken in one-hour increments. Please see CCB intranet for policy details.

LEAVE OF ABSENCES

Bereavement Leave

Bereavement leave allows an employee to receive paid leave because of the death of a close relative up to five (5) days. In order to allow employees to attend funeral or memorial services and help with family adjustments following the death of an immediate family member, employees are eligible for up to (5) five days of absence with pay. Immediate family includes parents, spouse, registered domestic partner, children, brothers, sisters, mother-in-law, father-in-law, grandparents, or grandchildren. Any exceptions will be made at the discretion of Human Resources.

Family and Medical Leave

Under The Family and Medical Leave Act (FMLA) an employee is eligible once they have worked for CCB for one year and a minimum of 1,250 hours over the previous 12 months. They are then eligible to take up to 12 weeks of unpaid, job-protected leave in a rolling 12- month period for the following family and/or medical reasons:

- For the care of the employee’s child within one year of her/his birth or placement for adoption or foster care
- For the care of the employee’s spouse, child, stepchild, parent, parent-in-law, or grandparent who has a serious health condition
- For a serious health condition that makes the employee unable to perform the essential functions of the job

The 12-month period used for calculating leave eligibility will be the 12 months rolling backward from the date of the requested FMLA leave.

Employees must provide CCB with 30 days of advance notice when the need for leave is foreseeable. Employees may be required to submit a health care provider’s statement verifying the need for Family Leave, the beginning and expected ending dates, and estimated time required.

During Family Leave, CCB will continue to provide the employee with medical coverage under its group health plan. If the employee is covering dependent(s) they must continue to make the monthly premium payments to CCB in order to continue their medical coverage during the leave. While on unpaid leave employees will not accrue universal leave or any other benefit, nor will they receive holiday pay. Also, if the employee chooses not to return to work after the leave for reasons other than the continuation, onset, or recurrence of a serious health condition CCB may ask to be reimbursed for the company paid coverage during the leave.

If the employee is entitled to universal leave pay, such paid leave must be exhausted prior to unpaid FMLA leave.

All time off that meets the FMLA eligibility criteria, including time off because of on-the-job injuries (Workers' Compensation), will be classified as family and medical leave under this policy and will count toward entitlement to leave.
An employee on FMLA leave is requested to provide CCB with at least two weeks' notice of the date the employee intends to return to work, if applicable the employee must provide a return-to-work notice from their physician. Upon return from Family Leave, the employee will be reinstated to the same position or to an equivalent position for which the employee is qualified.

Family Leave Due to a Call to Active Duty

This benefit provides 12 weeks of FMLA leave due to a spouse, son, daughter, or parent being on active duty or having been notified of an impending call or order to active duty in the Armed Forces. Leave may be used for any "qualifying exigency" arising out of the service member's current tour of active duty or because the service member is notified of an impending call to duty in support of a contingency operation.

Military Family Leave

During a period of military conflict, CCB provides eligible employees with up to 15 days of unpaid leave to be with their military spouse who is notified of an impending call or order to active duty, or who has been authorized for leave from deployment.

To be eligible for this benefit, you must be employed an average of 20 or more hours per week. You must notify your direct supervisor of your intention to take the leave under this policy within 5 business days following receipt of the official military notice.

You may choose to apply applicable accrued paid leave benefits while taking military family leave.
Health insurance benefits may continue at the level and conditions as provided under applicable laws.
Upon the completion of your leave, you may return to your original position or an equivalent job, *i.e.,* equivalent pay, benefits, and conditions of employment.

Caregiver Leave for an Injured Service Member

This benefit provides 26 weeks of FMLA leave during a single 12-month period for a spouse, son, daughter, parent, or nearest blood relative caring for a recovering service member. A recovering service member is defined as a member of the Armed Forces who suffered an injury or illness while on active duty that may render the person unable to perform the duties of the member's office, grade, rank, or rating. This form of leave also applies to eligible family members of veterans for up to five years after the veteran leaves service for a serious illness or injury incurred during active duty.

Employees can utilize the leave on an incremental basis or in the smallest increment that the employer's payroll system tracks under both of these leave requirements.

In compliance with State laws, available leave under this policy may be taken in addition to the actual time period a woman may need for time off due to her temporary disability related to pregnancy or childbirth. Further, approved time off to care for domestic partners will not count under the federal Family and Medical Leave Act (FMLA), because the FMLA does not include domestic partners in the definition of immediate family members. This form of leave relates only to coverage under State Family Leave Act.

Maternity Leave

Pregnancy disability leave is granted to all pregnant employees upon receipt of a physician's certification stating that they are unable to work due to pregnancy. Employees on leave are expected to keep the company posted regarding expected return date.

An employee on authorized pregnancy disability leave will return to the job she left unless the company is unable to return the employee because of business necessity. If this is necessary, the employee will be offered the first available job of like status and pay, or if none is available, a job of lower status and pay. If an employee chooses to wait for the first job of like status and pay, this reinstatement right will continue for one year.

We will provide nursing mothers with sufficient work shift modifications and private space to express milk.

Domestic Violence Leave

If you or your family member (child, spouse, domestic partner, parent, parent-in-law, grandparent, or person with whom you have a dating relationship) are a victim of domestic violence, sexual assault or stalking, CCB may offer a reasonable period of leave (as determined by CCB), intermittent leave or a reduced schedule to seek legal or law enforcement assistance, counseling or medical treatment.

Leave is without pay unless you choose to use accrued sick time. You will be asked for written verification of the need for leave. We may also request documentation to determine family relationship. To the extent allowed by law, your health insurance benefits will continue at the level and conditions that would have been provided had you remained continuously employed. Upon completion of your leave, you may be restored to the same job or an equivalent position with equivalent pay, benefits, and conditions of employment.

Information you provide to determine eligibility or continuation for this leave may only be disclosed by CCB if you request or consent to its disclosure, is responsive to a court or administrative order or as otherwise required by federal or state law.

During any continuous leave, CCB may disable employee user access to CCB computing systems and/or networks.

The above-mentioned leaves are only a brief summary of the various Leave Act(s). Please contact Human Resources for more details.

Jury Duty Leave

At CCB we support our employees' fulfillment of their civic duty by serving jury duty when called. Employees must provide their immediate manager and Human Resources with a copy of the jury summons as soon as possible upon receiving the summons.

Employees are eligible to receive regular pay less juror's compensation for the time away from work to serve on a jury up to a maximum of 80 hours pay per calendar year. Adequate proof of service must be provided in order to receive pay during an absence for jury duty. Upon return to work, the employee must provide Human Resources with verification from the court of the number of days served on the jury and the amount of juror compensation paid per day.

An employee is expected to report for work if, during the period of the summons, he or she is not required to sit on a jury and is able to work. If an employee is released from jury duty with at least four hours remaining in the workday, he or she should return to work for the remainder of the day.

Exempt employees, who are required to miss a portion of a work week due to jury duty or required attendance as a witness, will not have a salary deduction made for the work time missed.

TIMEKEEPING/PAYROLL

Timekeeping

Accurately recording time worked is the responsibility of every non-exempt employee. Federal and state laws require CCB to keep an accurate record of time worked in order to calculate employee pay and benefits.

Non-exempt employees should accurately record the time they begin and end their work, as well as the beginning and ending time of each meal period in the payroll time keeping system. If a meal period is not taken or is interrupted with required work duties, this should also be documented in the payroll time keeping system. They should also record the beginning and ending time of any split shift or departure from work for personal reasons. Overtime work must always be approved before it is performed.

Altering, falsifying, tampering with time records, failing to accurately complete time records or recording time on another employee's time record may result in disciplinary action, up to and including termination of employment.

Non-exempt employees should report to work no more than 5 minutes prior to their scheduled starting time nor stay more than 5 minutes after their scheduled stop time without express prior authorization from their supervisor.

Exempt employees are not required to record their time in and out daily; however, they are responsible for submitting Time Off requests into the payroll time keeping system for approval by their manager.

Paydays

All employees are paid semimonthly on the 15th and last day of the month. Exempt employees' paychecks will include earnings for all work performed for the current pay period and any exception pay from the previous payroll period. Non-exempt employees' paychecks will include earnings for all work performed for the previous payroll period and holiday, vacation, and sick pay from the previous payroll period.

Employees will have pay directly deposited into their bank account. Employees will have access to the payroll provider's self-service web site to receive an itemized statement of wages and deductions. In the event that a regularly scheduled payday falls on a non-business day, such as a weekend or holiday, employees will be paid on the business day prior to the weekend or holiday.

Improper Payroll Deductions

It is our policy to comply with the salary basis requirements of the Fair Labor Standards Act (FLSA). Therefore, we prohibit any improper deductions made from the salaries of exempt employees.

Exempt employees who believe that any improper deduction has been made to their salary should immediately report this information to their direct supervisor, or to the Human Resources Department. Reports of improper deductions will be promptly investigated. Employees should notify the HR/Payroll of any suspected error as soon as possible and if it is determined that an improper deduction has occurred, we will make every attempt to adjust the error no later than your next regular pay period.

WORK CONDITIONS & HOURS

Performance Reviews

CCB promotes the success of every employee. CCB is committed to a system of ongoing performance feedback through coaching and counseling, employee performance reviews and assessments. Coaching sessions may be completed on a schedule determined appropriate or necessary by the Manager or at any time that an employee's performance falls below acceptable standards.

The job performance of each employee shall be evaluated on the basis of the job description, productivity goals established by management, and the experience and training of the employee. Factors that may be considered in the performance review include attainment of goals, knowledge of the job, quantity and quality of work, promptness in completing assignments, cooperation, initiative, reliability, attendance, judgment, attitude, and acceptance of responsibility.

Salary increases may or may not be given during the performance evaluation process or on an annual basis.

Remote Work Arrangements

From time to time, we may have Remote Work Arrangements with employees. Please refer to the separate Remote Work Agreement for details and stipulations pertaining to this policy. You may also refer to your manager or HR if you have further questions about Remote Work Arrangements.

Workplace Safety

CCB observes all applicable health and safety regulations under local, state, and federal laws, including OSHA. We also maintain a non-smoking and drug-free environment.

Employee safety and well-being, and that of our clients and customers are of the utmost importance. You can help prevent accidents and injuries by using good judgment.

Any accidents in the office or workplace concerns involving employees, clients, or guests should be reported immediately to your manager or Human Resources.

OVERTIME

Non-exempt staff will be paid at the rate of one and one-half times the regular rate of pay for time worked in excess of 40 hours in any one week. A work week begins on Sunday at 12:01 AM and ends with Saturday 12:00 midnight. Paid holidays, sick leave, and vacation are not included as hours worked for the purpose of determining overtime pay.

Work assignments and scheduling should be coordinated so that regular overtime work is not necessary. Employees should not work before the beginning or after the end of their regular shift unless it is necessary to properly serve our customers and it has been specifically requested or approved by management. Any overtime must be pre-approved by your manager.

BUSINESS TRAVEL EXPENSES- DOMESTIC

Airlines

Employees should purchase non-refundable airline tickets and purchase them a minimum of 7-14 days in advance of the travel departure date whenever possible. Employees must travel Economy/ Coach Class unless authorized in writing by management.

Hotels

Reimbursement for lodging is limited to the single standard room rate. No upgraded room category will be reimbursed without management approval. Expenses for staying in a private home (e.g., family, friends) in lieu of hotel costs are not reimbursable.

Car Rental

Employees should rent a midsize or smaller vehicle whenever possible. Cars should be refueled before returning to avoid fuel surcharges whenever possible. Insurance must be declined as it is covered in our company policy.

Frequent Flyer/Frequent Guest Programs

Employees may retain program awards and benefits. Participation in these programs should not influence flight or lodging selections in any manner that would result in increased costs to CCB.

Allowable Expenses

The following items may be reimbursable to employees when necessary and reasonable, and incurred while conducting CCB business. Reimbursable items include but are not limited to:

- Commercial airfare and surface transportation (Economy/Coach Class) including parking fees and tolls
- Actual gratuity tips paid, when reasonable and customary
- Hotel/lodging
- Meals incurred during out-of-town trip
- Hotel and Airline high-speed Internet connection

Non-allowable items (without management approval) include but are not limited to:

- No-show fees for hotels, airfare, or car rentals
- Cancellation fees except those unavoidable due to business requirements
- Class of service upgrades
- Barber, hair stylist, manicurist, spa services, shoeshines, and other grooming/personal service expenses
- Lost or stolen personal items
- Personal entertainment including movies and DVD rentals

- Traffic/parking violations
- Family member or other non-business associate's expenses
- Credit card fees including annual or membership fees, late fees, and interest charges
- Insurance premiums
- Clothing purchases
- Laundry and dry cleaning unless trip exceeds 5 business days
- Membership fees (including frequent flyer/frequent guest programs)
- Trip or flight insurance
- Pet care or kennel costs
- Babysitters or house-sitters

Travel Policy – International

Any employees traveling internationally for business will need pre-approval from their manager for all major expenses, including (but not limited to) airline fees, hotel, documents, etc.

CORPORATE CREDIT CARD GUIDELINES

CCB issues Corporate Credit Cards to certain employees for the payment of approved business expenses. Corporate Credit Cards are issued with Human Resources approval as a mutual convenience and may be withdrawn at any time. The department manager and Human Resources will determine if there is a need for the employee to be issued a Corporate Credit Card.

Corporate Credit Cards are to be used for authorized business expenses only. Unauthorized charges on your corporate credit card may be grounds for disciplinary action. Employees are responsible for all unauthorized charges. In the event that an employee is terminated, any outstanding unauthorized charges will be deducted from their final paycheck. CCB reserves the right to require immediate payment in full of any outstanding unauthorized debt.

VISITORS IN THE WORKPLACE

To provide for the safety and security of employees and the facilities at CCB, and for confidentiality of CCB and customer information, only authorized visitors are allowed in the workplace. Family and friends of employees are discouraged from visiting. Restricting unauthorized visitors helps maintain safety standards, protects against theft, ensures security of equipment, protects confidential information, safeguards employee welfare, and avoids potential distractions and disturbances. If an unauthorized individual is observed on CCB's premises, employees should immediately notify their manager or, if necessary, direct the individual to the main entrance.

INFORMATION SYSTEMS

This policy is intended to address use of company information systems, including but not limited to personal computers, internet, e-mail, software, telephones, and voicemail systems. Because telephones, voicemail, personal computers, and e-mail systems are provided by CCB for business use, all messages sent by or received on those systems are company documents. CCB reserves the right to access and disclose the messages that you send or receive on the voicemail, text, or email systems. Employees should also be aware that "deleted" messages from the computer screen might not actually be deleted from the e-mail system. Employees who abuse these policies and standards may be subject to disciplinary action up to and including termination.

Personal Computers

Each employee may be granted access to a bank-owned computer (PC, laptop, tablet, smartphone). Employees should not have any expectation of privacy with respect to the computer. As otherwise permitted by law, employees' activities may be monitored at any time without notice and CCB may monitor, listen to, read, copy, retain or record any messages, communications, data, or records created by, stored on, accessed by, or otherwise using CCB's computers. Employees who use the computers are therefore advised of this potential monitoring and agree to this practice.
On a daily basis, employees are responsible for maintaining the physical condition of their PC and reporting any software or hardware problems to the IT Department.

EMPLOYEES ARE PROHIBITED FROM LOADING OR INSTALLING UNAUTHORIZED SOFTWARE OR HARDWARE ON ANY COMPUTER SYSTEM; PROVIDED BY CCB, INCLUDING BUT NOT LIMITED TO PC'S, LAPTOPS, PERSONAL COMPUTER TABLETS, SMARTPHONES.

Employees will log off their PC every night. To avoid disruption in updates, employees shall not shut down their PC overnight.

Bank employees must not allow any third parties, known or unknown, to utilize the Bank's computer systems unless approved by Executive Management or the IT Department.

Employees are reminded that sensitive bank and customer information will be visible on PC screens. When necessary, monitors may be shut down to ensure the confidentiality of information. The blank screen saver is to be set up to run at an idle time of no more than 10 minutes.

Local Network Usage

CCB's systems and equipment, along with its associated hardware and software, are for official and authorized purposes only. Employees must use the local network only for official Bank business and access only files and data that are their own, that are publicly available, or to which they have authorized access. Employees should not have any expectation of privacy with respect to the above systems and equipment. As otherwise permitted by law, including but not limited to security and/or network management reasons, employees' activities may be monitored at any time without notice and CCB may monitor, listen to, read, copy, retain or record any messages, communications, data, or records created by, stored on or otherwise using the above systems and equipment. Employees who use these systems and equipment are therefore advised of this potential monitoring and agree to this practice.
Access to computer systems and networks owned or operated by CCB imposes certain responsibilities and obligations on Bank employees and is subject to local, state, and federal laws.

Users are instructed to protect their USERID and PASSWORD from unauthorized use. Sharing user credentials between employees is strictly prohibited unless authorized by the IT department.

Software will be installed only from approved internal servers to limit exposure to contaminated software. No software will be downloaded from the Internet onto any computer unless authorized by the IT department upon approval by management.

Requests to install application software must be approved by Senior Management. The IT Department will coordinate the installation of approved software. Software configurations will be scanned periodically to validate that no extraneous software has been added to a computer.

Users are to store all documents on the network file server for daily backup. No documents should be stored on the user's local hard drive. The IT Department may review any or all local drives from time to time to ensure compliance.

Employees should report any problems and/or performance drops on the network to the IT department. The IT Department will review all logs and reports to determine the cause and initiate repairs.
Employees may be subject to the limitation on their use of the networks as determined by the appropriate supervising authority.

Use of network services provided by CCB may be subject to monitoring for security and/or network management reasons. Employees who use these services are therefore advised of this potential monitoring and agree to this practice.

Employees who violate any copyright declarations are acting outside the course and scope of their employment or other authority and CCB is relieved of any legal responsibility thereof. Employees will be personally responsible and liable for such infringing activities.

By participating in the use of networks and systems provided by CCB, employees agree to be subject to and abide by this policy for their use.

Willful violation of the principles and provisions of this policy, misuse of CCB's network systems or equipment and/or use of the systems or equipment that otherwise violates the provisions of this handbook, including but not limited to the equal employment opportunity and anti-harassment policies, may result in disciplinary action up to and including termination of employment.

Electronic Mail Usage

All CCB employees are to use electronic mail as they would with any other type of official Bank communications tool. This implies that when an e-mail is sent, both the sender and the reader should ensure that the communications comply with normal communications guidelines.

CCB's primary purpose in providing employees with access to e-mail is to conduct business communications. Only authorized e-mail software may be used for bank business. Employees should not have any expectation of privacy with respect to accessing personal email from CCB systems. Employees found to be deliberately misusing e-mail will be disciplined appropriately, up to and including termination of employment.

All electronic messages created and/or stored on Bank owned or a third party contracted systems are the property of CCB and are not considered private. Employees should not have any expectation of privacy with respect to any electronic messages that are accessed, created, or stored using CCB or third party contracted systems. CCB reserves the right to monitor, review, copy, retain and record all employee e-mail communications and any related communications, data, or records. Incoming and outgoing email communications will be processed and retained in an email archive prior to sending and receiving. CCB may retrieve e-mail messages and related communications, data, or records even though the sender and the reader have deleted them. Such messages may be used in disciplinary actions up to and including termination of employment.

To protect CCB's systems from possible infection or destruction by viruses or other harmful devices, employees may not download or open any e-mail attachments (exceptions would be common file formats like Word, Excel, or PDF files from a known source) from unknown untrusted sources without approval

and/or technical assistance from the IT Department. Installing or downloading any software/program is prohibited – except by authorized individuals with the approval of management.
By participating in the use of E-Mail services provided by CCB, employees and Bank agents agree to be subject to and abide by this policy for their use.

Willful violation of the principles and provisions of this policy, misuse of CCB's e-mail systems and/or use of the e-mail systems that otherwise violates the provisions of this handbook, including but not limited to the equal employment opportunity and anti-harassment policies, may result in disciplinary action up to and including termination of employment.

CCB may choose to revoke access to e-mail by Bank employees at any time, with or without notice and for any reason whatsoever. In order to monitor whether an e-mail is being used in a manner consistent with CCB's policy, CCB reserves the right to monitor incoming and outgoing e-mail.

All emails sent from the Bank must contain the following message:

> *The information in this message is intended only for the addressee or the addressee's authorized agent. This message may contain information that is privileged, confidential or otherwise exempt from disclosure. If the reader of this message is not the intended recipient or that person's authorized agent, then you are notified that any dissemination, distribution or copying of this message is prohibited. If you have received this message in error, please notify the sender by return e-mail or destroy any copies of this message.*

All emails sent from any loan originating or support functions must contain the following message:

> *CCB's agreement and commitment to lend money is contingent on the Bank's final underwriting approval and proper documentation. Commitments to lend money must be in writing and signed by an authorized CCB representative. Any loan terms addressed in this email are subject to change and final documentation. Nothing contained in this email is to be considered a commitment to lend money or extend credit.*

All electronic messages and transmissions which contain sensitive non-public data must be sent using industry-standard secure encryption. Failure to adhere to secure transmissions could lead to the loss of sensitive bank data and may result in disciplinary action which could even lead to termination of employment.

The bank will provide secure systems and train employees on the proper usage of these systems to ensure correct sending of sensitive non-public data.

Internet Usage

CCB's communications systems and equipment, including Internet systems, along with their associated hardware and software, are intended for official and authorized purposes. Managers may authorize incidental personal use which: does not interfere with the performance or professional duties; is of reasonable duration and frequency; does not overburden the system or create any additional expense to CCB and does not violate any other provision of this handbook, including but not limited to the equal employment opportunity and anti-harassment policies. CCB has implemented systems to monitor and restrict the personal usage of the internet.

Employees may be subject to the limitation on their use of the Internet as determined by the appropriate supervising authority.

Employees should not have any expectation of privacy with respect to the above services. As otherwise permitted by law, including but not limited to security and/or network management reasons, employees' activities may be monitored at any time without notice and CCB may monitor, listen to, read, copy, retain or record any messages, communications, data, or records created by, stored on, or otherwise using CCB's Internet services. Employees who use these services are therefore advised of this potential monitoring and agree to this practice.

All users who require access to Internet services must do so by using Bank approved software and Internet gateways.

No software is to be downloaded from the Internet onto any computer unless authorized by the IT department upon approval from management.

By participating in the use of Internet services provided by CCB, employees agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy, misuse of CCB's Internet systems and/or use of the Internet systems that otherwise violates the provisions of this handbook, including but not limited to the equal employment opportunity and anti-harassment policies, may result in disciplinary action up to and including termination of employment.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a CCB network, such as those behind Enterprise Teleworker (ECT) or VPN, must adhere to the following:

- Enable Wi-Fi Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Change the default SSID name
- Change the default login and password

SOCIAL MEDIA GUIDELINES AND POLICY

CCB recognizes that Social Media tools such as apps, blogs, and other digital channels established for online interaction and connection are a normal part of daily life for many people. CCB has a Social Media Guidelines and Policy (“Policy”) which applies to CCB’s official use of Social Media for marketing and promotion, as well as employees’ use of social networking sites both at work and outside of work. The purpose of this Policy is to establish standards and expectations regarding any CCB related use of Social Media. This Policy can be found on the CCB Intranet in the Policies section under "Other". Employees must familiarize themselves with the Policy and abide by its guidelines and directives. Violations of the Policy may subject an employee to disciplinary action or other remedial measures up to and including termination of employment.

MOBILE DEVICE POLICY

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to use a personal or CCB issued mobile device that can access the

Banks' electronic resources. This mobile device agreement applies to, but is not limited to, all devices and Bank media that fit the following device classifications:

- Laptop/Notebook
- Tablet computers such as iPads
- Mobile/cellular phones
- Smartphones
- PDAs
- Any mobile device capable of storing Bank data
- Mobile Wi-Fi Hotspot

Applicability

This policy applies to all CCB employees, including full and part-time staff, who use a mobile device to access, store, back up, or relocate any bank resources/info. Such access to the bank's resources/info is a privilege, not a right. Consequently, employment at CCB does not automatically guarantee mobile access to CCB electronic systems.

Eligible Employees

Mobile device issuance must be approved by a member of the Sr. Management Team. The approval is based on the following business needs criteria:

- An employee who is responsible for emergency matters where they must be available 100 percent of the time.
- An employee's job effectiveness will show a significant increase through the use of a cell phone or electronic access/device.
- A group of employees has the need for group or shared devices for purposes such as rotating on-call contact.
- An employee is not normally present at a fixed workstation and timely communication is difficult to transact.
- An employee is required to make frequent and/or prolonged travel outside the office.
- Employees may not use their personal or work assigned device for work purposes during periods of unpaid leave without authorization from management.

CCB reserves the right to deactivate the company's application and access on the employees personal or bank owned device during periods of unpaid leave.

Non-Exempt Employee Use

Nonexempt employees may not use their personal device or bank owned device for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending, and responding to emails or text messages, responding to phone calls, or making phone calls.

General User Responsibility

Employee agrees to a general code of conduct that recognizes the need to protect confidential data that is stored on or accessed using a mobile device. This code of conduct includes but is not limited to:

- Ensuring the physical security of the device at all times.
- Maintaining the software configuration of the device – both the operating system and the applications installed.

- Preventing the storage of sensitive Bank data in unapproved applications on the device.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes.
- Reporting a lost or stolen device immediately.
- Maintaining a back-up of personal data, such as contacts, pictures, videos, and music stored.

Bank-Owned Mobile Devices

All Bank-owned mobile devices will be managed by the CCB Information Technology Department, according to the standards below:

- All devices must be encrypted to protect data should the device become lost or get stolen.
- The Department will enforce a device PIN lock with a minimum of 6 digits, as well as enabling the remote wiping feature that will be initiated upon the loss, trade-in, or other disposition of the device, or the termination of the employment relationship with the individual to which the device has been assigned.
- Employees are solely responsible for backing up any personal data on the device. The Bank is not responsible for the loss of any personal data such as pictures, contacts, or other items that may occur as a result of the enforcement of any security policy or procedure, or any other reason.
- The Bank may at its discretion restrict which apps or other software may be installed or used on the device. Further, the Bank may prevent devices that have been "rooted," "jail broken," or otherwise modified from connecting to its network.
- The employee must notify the Information Technology Department immediately if the device is lost or stolen.
- The employee must notify IT prior to the sale, upgrade, or trade-in of the device.

Technical Support of Bank-Owned Mobile Devices

The Information Technology Department will provide support and guidance for the installation and connection of the device to the Bank's infrastructure and network resources as well as basic device support. Hardware and more advanced technical issues will be facilitated by the IT Department, who may escalate the support request to a third party or direct the employee to contact the carrier for carrier related issues.

Employee-Owned Mobile Devices

If the device sends and receives bank communications, all employee-owned mobile devices may be monitored or reviewed from time to time by the CCB Information Technology Department. All employees who choose to receive Bank email on their mobile device(s) agree to the following:

- All devices must be encrypted to protect data should the device become lost or get stolen.
- Employees will not permanently store sensitive business data on the device outside of the email application or other approved secure storage container.
- The IT Department will enforce a device PIN lock with a minimum of 6 digits, as well as enabling the remote wiping feature that will be initiated upon the loss, trade-in, or other disposition of the device, or the termination of the employment relationship with the individual to which the device has been assigned.
- Employees are solely responsible for backing up any personal data on the device. The Bank is not responsible for the loss of any personal data such as pictures, contacts, or other items that may occur as a result of the enforcement of any security policy or procedure, or any other

reason.

- The employee will promptly install security updates and operating system updates released by the device manufacturer or mobile carrier.
- The employee will not “jailbreak” or “root” their devices or in any way circumvent the built-in device security mechanisms.
- The employee will allow the installation and configuration of a mobile device management agent, or security-related software, as necessary.
- The employee must notify the IT Department immediately if the device is lost or stolen.
- The employee must notify the IT Department prior to the sale, upgrade, or trade-in of the device.
- The Bank is under no obligation to maintain support for any particular make or model of device and may terminate support for existing devices at its discretion for any reason, including but not limited to security concerns with a device or operating system, changing Bank technical standards that render a device incompatible with new or enhanced features, or obsolescence.

Technical Support of Employee-Owned Mobile Devices

The Information Technology Department will provide support and guidance for the installation and connection of the device to the Bank’s infrastructure and network resources. All other support-related issues must be directed to the mobile carrier service provider or other qualified professional.

Personal Use

Personal use is permitted with internet limitations on Bank owned devices. Employees are subject to all bank policies, in particular, the Bank’s Internet Use Policy, Acceptable Use Policy and Information Security Policy.

Security & Monitoring

The employee is responsible for complying with security controls put in place by CCB. The employee is responsible for ensuring the security of their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is strictly prohibited. Employee is forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.

Security and configuration requirements:

- Wi-Fi internet access must be password protected. The Employee must agree to never use an open public Wi-Fi connection to access the internet.
- Upon instruction from the Technology Department, the device operating system software will be updated & kept current.
- All mobile devices will be configured to encrypt the content.

Bank Right to Monitor and Protect

The Bank has the right to, at will:

- Monitor bank messaging systems and data including data residing on the user’s mobile device. This includes but is not limited to text messages, emails, call logs, photos, videos, etc.
- Modify, including remote wipe or reset to factory default, the registered mobile device configuration remotely. (Personal data, as described above, will be lost if not backed up).

Applications/Downloads

Only applications available in the Apple App Store or Google Play Store are permitted to be used and downloaded onto the employee's mobile device. CCB will only allow designated employees to access Bank information with the following applications on approved devices:

- Exchange Email, Calendar, and Contacts via Active Sync for Exchange Platform.

Passwords

It is required that all mobile devices be password or PIN protected. Employees are required to know what their password or PIN is and to not distribute to anyone. If an employee forgets their password or PIN, the employee will need to contact the CCB IT Department and have their device wiped. Wiping the device may cause all pictures and contact information to be lost (unless they are backed up). The Technology Department does not have the ability to reset mobile device passcodes.

Lost, Stolen or Damaged Device or Components

If a bank owned mobile device or any of its components is lost, stolen or damaged, the employee is responsible for contacting the CCB IT Department immediately. If a replacement device or component is available, it will be reissued to the employee. Replacement devices and components may be used or refurbished devices.

If a replacement device or component is not available, and the incident was a result of poor care or negligence, the employee will be responsible for the device's replacement.

Driving Safely

Employees are prohibited from using Bank issued mobile devices while driving, and strongly discourage the use of a mobile device while conducting business and driving. Before using a mobile device while driving, employees are expected to pull off to the side of the road and safely stop the vehicle. It may be acceptable to use Bluetooth for speaking appointments, however it's prohibited to be engaged in a video call for business purposes while driving. Employees are expected to abide by all applicable laws covering the use of Bank issued or personally owned mobile devices while driving regardless of whether the vehicle is a Bank-Owned vehicle.

CL to IL (Corporate Liable to Individual Liable)

It is the Bank's policy that the wireless numbers associated with all Bank issued Smartphone and Cell Phone devices are Bank owned. There will be no approval granted to an employee to seize their wireless number upon separation from the Bank. Employees may elect to transfer their personal number to the Bank issued mobile device. If an employee that transferred their personal number to the Bank separates from the Bank and wishes to transfer their number back to a personal device, approval will not be granted.

Employee Termination

If employment is terminated all bank owned mobile devices and their components must be returned to CCB.

Policy Authority and Enforcement

The Bank's SVP of IT is responsible for the development and oversight of these policies and standards. The SVP or IT works with Senior Management, Human Resources, the Information Security Officer, Audit Services, Compliance, Legal, and others for development, monitoring and enforcement of these policies and standards.

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services, or relationship with the Bank and/or action in accordance with local ordinances, state, or federal laws.

DRIVING ON COMPANY BUSINESS

CCB considers safe driving practices to be a vital part of our operation. It is important for the safety of our employees and other drivers on the road. The purpose of this policy is to ensure the safety of those individuals who drive their own vehicles on company business. It is the driver's responsibility to operate the vehicle in a safe manner and to drive defensively to prevent injuries and property damage. CCB expects each driver to drive in a safe and courteous manner pursuant to the following policy.

Use of mobile technology devices such as cellular phones, laptops, personal digital assistants, navigation systems, and portable digital audio and video players have been shown to distract drivers and can increase the risk of motor vehicle accidents. To help reduce the possibility of vehicle accidents in connection with the use of mobile technology, CCB has adopted a policy applicable to all employees while driving a company vehicle or any other vehicle (including rented, leased, borrowed, or personally owned vehicle) while conducting company business.

- Employees should comply with all federal, state, and local laws and regulations regarding the use of mobile technology devices including cellular phones. The Governors Highway Safety Association maintains a list of state and local restrictions on cellular phone use (www.ghsa.org).
- Use of handheld cellular phones while driving is prohibited.
- Cellular phone calls using hands-free technology while driving is discouraged. To minimize the impact of distraction, calls, if any, should be brief. Extended conversations should be made while not driving.
- Sending or reading text messages or e-mails, dialing cellular phones, viewing television, videos or DVDs and inputting data into laptop computers, personal digital assistants or navigation systems are prohibited while driving.

COMPANY OWNED VEHICLE USAGE

The CCB Company Owned Vehicle Usage Standard describes guidelines for employee use of company-owned vehicles. A "company vehicle" is any type of vehicle the company owns and assigns to employees to support their transportation while engaged in the business of CCB. Company cars are an asset to the company and ensuring proper use, care and operation is imperative for both asset protection and minimizing corporate liability. The Bank retains the right to revoke or assign company vehicles at its discretion.

Only qualified, insured, and employees authorized by Human Resources are permitted to use company vehicles. Human Resources defines qualified employees as follows:

- The employee must be at least 18 years old
- Employee must demonstrate a clean driving record, which will be verified by Human Resources prior to authorization
- A current copy of the employee's active driver's license is on file with Human Resources
- Enterprise Risk Management has added the employee to the Bank's corporate auto insurance policy

If an employee has their driver's license suspended or revoked, he or she must inform Human Resources and their Manager immediately and may be ineligible from driving a company vehicle in the future.

Employees who are fatigued and/or sick should avoid driving if they feel their driving ability is impaired. If sickness occurs during business travel that requires the use of a company vehicle, employees should take precautions to ensure safe operation of the vehicle.

Employees authorized to use a company vehicle must obey all traffic rules and wear a seatbelt while the vehicle is in operation. Hand-held cell phones (whether company-provided or personal) may not be used while operating the vehicle, though hands-free devices may be used as allowed by law. Employees that need to use their hand-held device must first pull off the road and turn off the ignition. All cell phone use, including talking, reading, typing, or sending a text message while at a stop sign, red light, or while stopped in traffic, is prohibited by law.

EMPLOYEE CONDUCT & DISCIPLINARY ACTION

Employee Conduct and Work Rules

Employee conduct and work rules apply to all employees working on-site at one of CCB buildings, or remotely with Manager approval. Please refer to the Remote Work Program for details on working remotely.

To ensure orderly operations and provide the best possible work environment, CCB expects employees to follow rules of conduct that will protect the interests and safety of all employees and the organization.

It is not possible to list all the forms of behavior that are considered unacceptable in the workplace. The following are examples of, but are not a complete list of, infractions of rules of conduct that may result in disciplinary action, up to and including termination of employment:

- Theft or inappropriate removal, possession, or damage of CCB or customer property or funds, or any failure to report or concealment of such activity
- Allowing or assisting an unauthorized person to enter a vault, teller counter or other area where cash or other valuables (including confidential customer information) are secured
- Falsification of or inaccurate or untimely maintenance of timekeeping, work, personnel or other company records, Falsification of or inaccurate or untimely maintenance of accounts or accounting information,
- Working under the influence of alcohol or illegal drugs
- Possession, distribution, sale, transfer, or use of alcohol or illegal drugs in the workplace, while on duty, or while operating employer-owned vehicles or equipment
- Fighting or threatening violence or other intimidating behavior in the workplace
- Negligence or improper conduct leading to damage of employer-owned or customer-owned

property
- Insubordination or other disrespectful conduct
- Dishonesty or other failure to maintain the highest standards of integrity or ethics
- Participation in business directly competing with the company
- Violation of safety or health rules
- Sexual or other unlawful or unwelcome harassment or discrimination
- Possession of dangerous or unauthorized materials, such as explosives or firearms, in the workplace or while performing Bank business
- Excessive absenteeism or any absence without notice
- Unauthorized absence from workstation during the workday
- Unauthorized use of telephones, mail system, e-mail, network, Internet or other employer-owned systems or equipment
- Unauthorized use or disclosure of business "secrets" or business or customer confidential or sensitive information
- Violation of personnel policies included in this Handbook or elsewhere, including but not limited to the Code of Conduct
- Violation of any laws, rules, regulations, or standards applicable to CCB or the banking industry
- Unsatisfactory performance or conduct
- False statements on an employment application or related background check requests
- *Employees are required to report to Human Resources any misdemeanor or felony conviction within 5 days of the conviction.*

Employment with CCB is at the mutual consent of CCB and the employee, and either party may terminate that relationship at any time, with or without cause, with or without reason and with or without advance notice.

Discipline Process

When an employee demonstrates unsatisfactory performance or behaves in a manner that may negatively affect the operations of the organization it is important that prompt and appropriate action be taken by the manager. Taking swift action supports an open and productive work environment.

In most cases of performance or behavioral problems a warning, will begin and escalate from there to ensure that expectations are understood and to allow the employee the opportunity to improve his or her performance or behavior. In some circumstances immediate termination or other discipline may be appropriate. CCB is an at-will employer. This means that the company or the employee may terminate employment at any time with or without reason. The discipline process does not imply a contract and employment may be terminated at any time during a discipline process.

Verbal Warning

This allows the manager to discuss the perceived problem directly with the employee. This is usually the first step in a disciplinary process but may be avoided depending on the severity of the discipline problem.

Written Warning

When a problem continues, escalates, or there is a reoccurrence of the problem or a similar problem, a written warning may be issued. Both the manager and the employee will sign any written material related to the procedure. The employee will receive a copy of the signed material and a copy will be placed in their HR file. This is usually the second step in a disciplinary process but may be avoided depending on the severity of the discipline problem.

Final Written Warning
If the problem continues, escalates, or if there is a reoccurrence of the problem or a similar problem it may be necessary to issue a final written warning. It is imperative that the employee understands clearly that another breach of conduct or continued unsatisfactory performance may result in termination. This is usually the final step in a disciplinary process but may be avoided depending on the severity of the discipline problem. Any and all documentation related to the matter will remain in the employee's HR file.

Involuntary Termination
If an employee has failed to improve his or her performance and/or behavior employment may be terminated. This step may occur after disciplinary steps have been taken and the employee has failed to improve his or her performance and/or behavior. Termination of employment may also occur earlier in the discipline process or entirely outside of the discipline process in situations that warrant more severe or prompt action.

WORKPLACE VIOLENCE

Consistent with our efforts to provide a safe workplace, acts or threats of violence, regardless of whether they cause harm or damage, by or towards our customers, employees, or CCB property will not be tolerated on CCB premises or while conducting business. Acts or threats of violence include verbal attacks, aggressive or intimidating behaviors, threats and/or use of physical force or weapons.

Any act or threat of violence should be reported to your supervisor or manager and the Human Resources Department immediately. CCB expressly prohibits any form of retaliation against an employee for reporting information under this policy. Violations of this policy may result in disciplinary action up to and including termination of employment and notification to appropriate law enforcement agencies.

WORKPLACE SEARCHES

CCB reserves the right to use any lawful method of investigation it deems necessary to determine whether any person has engaged in conduct that interferes with or adversely affects business. A search does not imply an accusation of theft or that an employee has broken a company rule.

Employees entering and leaving the facility are subject to questions and search at the employer's discretion. Lockers, vehicles, and personal possessions on CCB premises will also be subject to search. This policy applies to all employees, including management. Failure to comply may result in termination of your employment.

HANDGUNS/FIREARMS

The possession of any handguns, firearms, explosives, or any other weapons by employees in the workplace, on CCB property, or while on CCB business activity is strictly prohibited.

If you witness the possession or concealment of any weapon, firearm, or explosive by another employee, report it to your manager, Security Officer, or Human Resources immediately.

SMOKING

In keeping with CCB's intent to provide a safe and healthful work environment, smoking (e.g., carrying or smoking of any kind of lighted pipe, cigar, cigarette or any other lighted smoking equipment), chewing

tobacco or snuff or any other use of tobacco products on CCB premises, at any entrance or exit, or as further prohibited by state or local law, is absolutely prohibited.

MEAL AND REST PERIODS

Each workday, full-time nonexempt employees (and other nonexempt employees as required by law) are provided with two (2) rest periods of at least ten (10) minutes each. Managers will advise employees of the regular rest period length and schedule. To the extent possible, rest periods will be provided in the middle of work periods. Since this time is counted and paid as time worked, employees must not be absent from their workstations beyond the allotted rest period time.

All full-time employees (and other nonexempt employees as required by law) are provided with one meal period of at least thirty (30) minutes each workday which commences no less than two hours or more than five hours from the beginning of the shift. Managers will schedule meal periods to accommodate operating requirements within these parameters. Employees will be relieved of all active responsibilities and restrictions during meal periods and will not be compensated for that time.

APPOINTMENTS

Your manager must approve time off during the day for personal appointments in advance. In general, consideration should be given to CCB's peak business hours when scheduling appointments.

DRUG AND ALCOHOL USE

It is CCB's desire to provide a drug-free, healthful, and safe workplace. To promote this goal, employees are required to report to work in appropriate mental and physical condition to perform their jobs in a safe and satisfactory manner.

While on CCB premises and while conducting business-related activities off CCB premises, no employee may use, possess, distribute, sell, or be under the influence of alcohol or illegal drugs. The legal use of prescribed drugs is permitted on the job only if it does not impair an employee's ability to perform the essential functions of the job effectively and in a safe manner that does not endanger other individuals in the workplace. If an employee is required to take prescription medication that may affect the employee’s ability to perform the functions of his/her job, the employee is required to advise management of the situation and, may request an appropriate and reasonable accommodation for the employee’s medical condition.

Violations of this policy may lead to disciplinary action, up to and including immediate termination of employment, and/or required participation in a substance abuse rehabilitation or treatment program. Such violations may also have legal consequences.

Employees with questions on this policy or issues related to drug or alcohol use in the workplace should raise their concerns with their supervisor or the Human Resources department without fear of reprisal or retaliation.

GRIEVANCE PROCEDURE

CCB is committed to providing the best possible working conditions for its employees. Part of this commitment is encouraging an open and frank atmosphere in which any problem, complaint, suggestion, or question receives a timely response from CCB supervisors and management.

If a situation occurs when employees believe that a condition of employment or a decision affecting them is unjust or inequitable, they are encouraged to make use of the following steps. Employees who have a complaint of unlawful harassment or discrimination must use the complaint procedure in the Anti-Discrimination and Anti-Harassment Policy. The employee may discontinue the procedure at any step.

- Employee presents grievance to immediate manager after incident occurs. If a manager is unavailable or an employee believes it would be inappropriate to contact that person, the employee may present the grievance to a member of executive or senior management.
- The member of management who receives the grievance from the employee will be responsible for responding to and/or resolving the grievance. As well as documenting the grievance, the discussion, and the steps taken to resolve the grievance and inform Human Resources of the grievance and resolution.
- If the grievance is still unresolved, the employee may present the grievance to Human Resources.
- Human Resources will counsel and advise the employee, assist in putting the grievance in writing, and visit with the employee's manager(s), if necessary. Human Resources will deliver the written grievance to the CEO for review and consideration.
- The CEO will inform the employee of the decision and forward the written response to *Human Resources* for the employee's file. The CEO has full authority to make any adjustment deemed appropriate to resolve the grievance.

Not every problem can be resolved to everyone's total satisfaction, but only through understanding and discussion of mutual problems can employees and management develop confidence in each other. This confidence is important to the operation of an efficient and harmonious work environment and helps to ensure everyone's job security.

SOLICITATION POLICY

The CCB Solicitation Policy prohibits certain solicitation and distribution activities on CCB premises, without prior authorization from management, as follows:

Employees may not solicit other employees during work times, except in connection with a Company approved or sponsored event. This includes, buying, selling, seeking contributions, and offering tickets or memberships (Working time is any time you are expected to be performing your duties, not including break periods or meal periods.)

- You may not distribute or post non-work-related materials in working areas or during work times, except in connection with a CCB sponsored event. Bulletin boards, CCB mail, electronic mail, and other communications channels on CCB premises are solely for business purposes, including information on employee policies, programs, and benefits.
  *(*Working areas are any place where the business of CCB is being performed, such as workstations, offices, conference rooms, photocopy rooms, etc.)
- Unauthorized non-employees are not permitted on CCB premises. Non-employees, whether authorized to be on premises or not, may not solicit CCB employees.

The following are some examples of, but are not intended as a complete list of, solicitation and distribution which are not permitted under the policy, during working time and in work areas:

- Posting notices for sale of personal articles
- Posting notices for room mates
- Distributing any kind of non-work-related literature, brochures, leaflets, pamphlets, notices, cards, advertising, etc.
- Having nonemployees solicit employees on Bank premises for any reason
- Sending chain letters

The sole exceptions to this policy are charitable and community activities supported and approved by CCB management and CCB sponsored programs related to CCB products and services.

ATTENDANCE & WORK SCHEDULES

Managers are responsible for establishing employee work schedules. Employees are expected to work the established schedule unless prior approval has been obtained from the manager.

If an employee is unable to report to work or will be tardy for any reason, he/she must notify his/her manager as soon as practicable prior to their scheduled start time. If the employee leaves a message for his/her manager prior to the opening of business, they must call in once the office opens and speak to his/her manager live. If their direct manager is not available, they must contact another member of the management team.

Excessive absenteeism/tardiness is unacceptable and may lead to a formal written warning and/or additional disciplinary action up to and including termination. If your absence or tardiness is due to an emergency, you must call in, or have someone call in for you, as soon as possible.

Attendance or tardiness problems that are not protected by leave laws, as well as failure to call in, may result in discipline up to and including termination. Any employee who fails to report for work or call in for two (2) days in a row, will be deemed to have abandoned their job and may be terminated.

PROFESSIONAL DRESS GUIDE

At CCB we strive for professionalism in all we do and believe dress, grooming and personal cleanliness affect the business image we portray to our customers and visitors.

We have adopted casual professional dress as our everyday dress standard. Our primary objective is that we project a professional image at all times. We will dress in a manner that is professional and respectful.

Clothing should present a neat, well-groomed appearance, suitable for daily business activities. We set a higher standard for ourselves and our appearance should be a point of pride.

All employees are accountable for exercising good judgment and ensuring they are dressed appropriately. Wearing inappropriate clothing will result in being sent home to change, returning in clothing that is appropriate. If this occurs, non-exempt employees will not be compensated for their time away.

Certain positions and departments may require employees to wear professional business attire based on customer and guest interaction.

Managers are charged with the responsibility of ensuring that their staff members' appearance is appropriate. Repeated violation will result in discipline, up to and including termination of employment.

Resignation

Resignation is a voluntary act initiated by the employee to terminate employment with CCB. Although advance notice is not required, CCB requests at least 2 weeks' written resignation notice from all employees.
Prior to an employee's departure, an exit interview may be scheduled to discuss the reasons for resignation and the effect of the resignation on benefits.

ATTACHMENT A- CODE OF CONDUCT

The policies in this Code of Conduct apply to all employees, officers and directors and set forth business ethics guidelines that specify the ethical and legal conduct expected of such individuals in a variety of identified business situations. These policies do not and cannot cover every situation involving ethical questions. Questions will arise concerning interpretation, intent, and application. Employees are encouraged to seek advice about any issues raised by these policies. From time to time a general notice will be issued regarding the application of certain sections of these policies. Advice and guidance may be obtained from any Senior Management member or the Human Resources Department.

Disregarding or failing to comply with any provision or policy in the Code of Conduct may result in disciplinary action, up to and including termination of employment.

THE BUSINESS OF CCB

The successful business operation and reputation of CCB and its affiliates is built upon the principles of fair dealing and ethical conduct of our officers, directors, and employees. Our reputation for integrity and excellence requires careful observance of the spirit and letter of all applicable laws and regulations, as well as a scrupulous regard for the highest standards of ethics, conduct and personal integrity.

The continued success of CCB is dependent upon our customers' trust and we are dedicated to preserving that trust. Employees owe a duty to CCB, its customers, and shareholders to act in a way that will merit the continued trust and confidence of the public.

CCB will comply with all applicable laws and regulations and expects its directors, officers, and employees to conduct business in accordance with the letter, spirit, and intent of all relevant laws and to refrain from any illegal, dishonest, or unethical conduct.

In general, the use of good judgment, based on high ethical principles, will guide you with respect to lines of acceptable conduct. If a situation arises where it is difficult to determine the proper course of action, you should discuss the matter openly with your immediate supervisor and, if necessary, bring the matter to the Chief Human Resource Officer for advice and consultation.

The following Code of Conduct specifies certain standards for the guidance of all officers, directors, and employees. Compliance with the Code of Conduct is the responsibility of every CCB officer, director, and employee. The Code should be considered as illustrative, but not regarded as all-inclusive.

CONFLICTS OF INTEREST

The purpose of these guidelines is to provide general direction so that officers, directors, and employees can seek further clarification on issues related to the subject of acceptable standards of operation. In

determining whether a conflict of interest could exist, officers, directors and employees should remember that the rules also apply to their spouses, adult children and other relatives or individuals in a similar relationship, where appropriate.

All officers, directors and employees should avoid situations which could result in, or give the appearance of, a conflict of interest concerning CCB, its business, its stockholders, or any affiliate or its customers. Personal interests which could affect the proper exercise of judgment must be avoided. In those cases where personal interests do exist, or may appear to exist, the officer, director or employee in question should disqualify him/herself and permit other members of CCB's staff to handle the transaction. All officers, directors and employees must disclose all potential conflicts of interest, including those in which they have been inadvertently placed due to either business or personal relationships with customers, suppliers, business associates, or competitors of CCB.

Transactions with outside firms must be conducted within a framework established and controlled by the executive level of CCB. Business dealings with outside firms should not result in unusual gains for those firms. Unusual gain refers to, but is not limited to, bribes, product bonuses, special fringe benefits, unusual price breaks, and other windfalls designed to ultimately benefit the employer, the employee, or both. Promotional plans that could be interpreted to involve unusual gain require specific executive-level approval.

An actual or potential conflict of interest occurs when an employee is in a position to influence a decision that may result in a personal gain for that employee or for a relative as a result of CCB's business dealings. For the purposes of this policy, a relative is any person who is related by blood or marriage, or whose relationship with the employee is similar to that of persons who are related by blood or marriage. Personal gain may result not only in cases where an employee or relative has a significant ownership in a firm with which CCB does business, but also when an employee or relative receives any kickback, bribe, substantial gift, or special consideration as a result of any transaction or business dealings involving CCB.

Having a business or other employment outside CCB is permissible provided that it does not conflict with the officer or employee's duties, or the time and attention required of his or her position at CCB. Also, the business or employment cannot be directly competitive with CCB or its affiliates and cannot otherwise violate Part 348 of the FDIC Rules and Regulations prohibiting a management official from serving two nonaffiliated depository organizations in situations where the management interlock likely would have an anticompetitive effect. However, if employees have any influence on transactions involving purchases, contracts, or leases, it is imperative that they disclose to an officer of CCB as soon as possible the existence of any actual or potential conflict of interest so that safeguards can be established to protect all parties.

Acceptance of membership on outside boards involves possible conflicts of interest. Officers, directors, and employees are encouraged to participate in civic, charitable, and other community organizations; however, participation in such organizations should be pre-authorized by appropriate management.

If you have any questions regarding this policy or a potential or present conflict of interest in violation of this policy, you should promptly contact the Human Resources department.

CONFIDENTIAL AND SENSITIVE INFORMATION

As a service organization dealing with private, sensitive, and confidential information, it is most important for us to treat all client information, account information and company information and all discussions regarding the same as confidential.

In the course of performing bank duties, employees may acquire confidential information about

customers, which is considered to be extremely sensitive. All information obtained by virtue of employment with CCB should be held in strictest confidence. This includes, but is not limited to, financial and personal or other sensitive information of customers, loan applicants or fellow employees (including personnel and payroll information), as well as CCB's financial information and information related to its internal affairs, competitive position, pricing and rates, strategic planning and dealing with its regulators. The following are specific examples of, but not a complete list of, confidential information:

- The identify of customers and potential customers and their personal, business, and financial information
- Non-public business and financial information of CCB
- Personal or non-public information regarding any employee of CCB
- Personal or non-public business information regarding any supplier, vendor, or agent of CCB
- Information related to, including the identity of, potential candidates for mergers and acquisitions
- Information regarding CCB's sales strategies, plans or proposals
- Information related to computer software programs, whether proprietary or standard
- Information related to documentation systems, network systems, information databases, customized hardware or other information systems and technological developments
- Manuals, processes, policies, procedures
- Compositions, opinion letters, ideas, innovations, inventions, formulas, and other proprietary information belonging to CCB or related to CCB's activities
- Security information, including without limitation, policies and procedures, passwords, personal identification numbers (PINs) and electronic access keys
- The terms, limits, premiums, conditions, and existence of certain corporate insurance policies
- Financial results of CCB
- Communications by, to and from regulatory agencies
- Certain communications with or from attorneys from CCB, whether internal or external
- Any other information which may be deemed confidential, or which may be otherwise protected

Proprietary, confidential, or other sensitive information must not be disclosed to any person except as required for authorized business transactions, as authorized by the customer, or as required by law. The information released must be within the parameters set forth in the authorization.

Employee discussions about customers must be limited to information required to provide a service to the clients. It is inappropriate to discuss customer affairs, accounts, files, or other customer information with other employees except on a need-to-know basis.

Information regarding both past and present employees is also considered confidential. All inquiries regarding past or present employees, including requests for employment references, must be referred to the Human Resources Department.

On a periodic basis, CCB is examined. The reports that examiners furnish must remain the property of the regulatory agency and are strictly confidential. Information contained in the reports is privileged information and should not be communicated to anyone not officially connected with CCB.

Financial information regarding CCB must not be released to any person unless it has been made available to the public in agreement with applicable disclosure regulations currently in effect. Exceptions to this general policy include disclosure to attorneys, accounts and other professionals working on behalf of CCB, as well as regulatory examiners. Any questions regarding disclosure of confidential financial information must be reviewed with and approved by the Chief Human Resource Officer or the Chief Digital Banking Officer, prior to disclosure.

Employees must refer all inquiries from the media to the attention of the Chief Digital Banking Officer of CCB. Employees must obtain prior approval from the Chief Digital Banking Officer or the Chief Human Resource Officer before discussing CCB's policies, procedures, or affairs with an outside party.

Confidential or other sensitive information pertaining to CCB or its customers, suppliers, stockholders, and employees is to be used solely for corporate purposes and must not be used for private interest or as a basis for personal gain by officers, directors, or employees.

In certain instances, confidential information could be considered “insider information” within the meaning of federal and state securities laws. Disclosure or use of such information for personal gain or for avoiding personal loss could result in substantial civil and criminal penalties to individuals who disclose or who use this information. Officers and employees must be extremely cautious in discussing the corporate affairs of CCB with its customers or with outsiders, including with stockholders or potential stockholders of CCB who a right to such information before an announcement do not have is made to all stockholders of CCB.

This section also applies to information inadvertently received by employees, including e-mails, facsimile transmissions, all types of mail, including inter-office mail, and all other forms of written, verbal, or electronic communications.

In addition, any CCB-related documents must be disposed of in the shred receptacle.

Officers and employees must comply with all internal control procedures established by CCB for the safeguarding of assets and proper reporting and disclosure of financial information. For more information, please refer to CCB’s Security Program as well as our Information Security Policy. You can find these policies in their entirety in the Public Drive “Policies” folder.

LEGAL AND TAX ADVICE

A client who seeks legal or tax advice from any CCB employee should be encouraged to consult with an attorney or an accountant. It is not appropriate for bank employees to try to provide clients with this type of advice. When recommending professionals, employees should not single out a particular firm but rather suggest at least three.

CUSTOMER REPRESENTATION BY EMPLOYEES

Employees are discouraged from acting as representatives for customers in conducting their banking business. CCB employees should not sign on customer accounts, have access to customer safe deposit boxes, or otherwise represent a customer without approval from the Chief Human Resource officer (CHRO).

CCB employees may, however, act in an ownership capacity or sign on the accounts of family members as previously defined.

BORROWING FROM CUSTOMERS

Employees are not allowed to request loans from individual or business banking customers. Granting or denying such requests imposes an inappropriate burden on the customer and could influence the employee's judgment or decisions. Any exemption from this rule must be approved by the CEO of CCB.

ENSURING THE INTEGRITY OF RECORDS

Records and accounting information must be accurate and maintained with reliability and integrity. Transactions must be reflected in an accurate and timely manner. False entries and activities that result in false entries are absolutely prohibited.

COMMISSIONS OR GIFTS FROM CUSTOMERS

The following regulation, taken from the Bank Bribery Act, 18 U.S.C. § 215, governing gifts and gratuities should be borne in mind of all bank employees, officers, and directors:

- Whoever corruptly gives, offers, or promises anything of value to any person, with intent to influence or reward an officer, director, employee, agent, or attorney of a financial institution in connection with any business or transaction of such institution; or
- as an officer, director, employee, agent, or attorney of a financial institution, corruptly solicits or demands for the benefit of any person, or corruptly accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business or transaction of such institution.
- shall be fined not more than $1,000,000 or three times the value of the thing given, offered, promised, solicited, demanded, accepted, or agreed to be accepted, whichever is greater, or imprisoned not more than 30 years, or both, but if the value of the thing given, offered, promised, solicited, demanded, accepted, or agreed to be accepted does not exceed $1,000, shall be fined under this title or imprisoned not more than one year, or both.

This includes special terms or price concessions obtained from any bank customer. It also includes but is not limited to indirect benefits, such as commissions, special discounts, free services, or any concessions from attorneys, insurance and real estate agents, brokerage houses and salesmen as an incentive for referring business to them.

Whether or not it violates the Bank Bribery Act, this policy also prohibits officers, directors and employees or members of their immediate family from soliciting, giving or accepting, whether for himself/herself or for a third party (other than CCB), cash, gifts, special accommodations, other favors or anything else of value from anyone in return for any business, service or confidential information of CCB or from anyone with whom the person is negotiating, soliciting or doing business with on behalf of CCB. Similarly, officers, directors and employees are prohibited from soliciting personal fees, commissions or other forms of remuneration or anything of value (other than bona fide salary, wages and fees referred to in 18 U.S.C. § 215(c)) because of any transaction or business involving CCB and are prohibited from accepting anything of value (other than bona fide salary, wages and fees referred to in 18 U.S.C. § 215(c)) from anyone in connection with the business of CCB, either before or after a transaction is discussed or consummated.

The preceding prohibitions are not applicable to (i) any bequest or gift that is based on family or personal relationship existing independently of any business of CCB, (ii) any benefit that is available to the general public under the same conditions on which it is available to the bank official; or (iii) any occasional gift (e.g., a business luncheon or the special occasion gift from a customer, but never cash), that, under the circumstances, is of nominal value (less than $100.00). The acceptance of gifts of more than a nominal value could be considered as an attempt at bribery and could subject both the giver and the recipient to felony charges as well as the penalties prescribed under the Bank Bribery Act. 18 U.S.C. § 215 as identified

above. The Bank Bribery Act also covers agents or attorneys of a financial institution.

It is against CCB's policy for an employee or immediate family member to keep a gift if the relationship between the donor and the employee was created through a transaction of bank business. This includes gifts given in a will or trust instrument. If the gift cannot be refused or returned, it must be donated to charity. If there is a question regarding donor-employee relationship or acceptance of a gift, it must be reviewed by the Chief Human Resource Officer.

Full and timely disclosure to a supervisor must be made with respect to any gifts (including hospitality and entertainment) received. Any question or doubt as to the appropriateness of their receipt should be referred to CCB's Human Resources department and/or the Chief Human Resource Officer.

CORPORATE ACTIVITY

CCB is prohibited by the Federal Election Campaign Act, 2 U.S.C. § 441b from making contributions or expenditures (gifts, loans, advances, deposits of money, or any services, or anything of value) which directly or indirectly are in connection with any Federal election to any political office, any primary election, or any political convention or caucus held to select candidates for any Federal public office.

CCB, therefore, does not condone the use of normal work hours of an employee to engage in activity, which directly or indirectly is in connection with any election to any political office, any primary election, or any political convention or caucus held to select candidates for any public office. However, this restriction does not apply to employees who use their non-working hours, including their break periods, for such activities.

DISHONEST ACTS AND ILLEGAL ACTIVITY

Officers, directors, and employees are expected to abide by all applicable local, state, and federal laws, regulations, and guidelines. Officers or employees engaged in activities found to be in conflict with and against these laws, regulations or guidelines, or who is convicted of committing an unlawful act on or off Bank premises, or whose conduct directly discredits CCB in any way, specifically including but not limited to crimes of dishonesty or a breach of trust or money laundering as described by Section 19 of the Federal Deposits Insurance Act (FDIA) is strictly prohibited.

As amended, Section 19 of the FDIA states:

(a) Prohibition

> **(1)** In general Except with the prior written consent of the [Federal Deposit Insurance] Corporation - **(A)** any person who has been convicted of any criminal offense involving dishonesty or a breach of trust or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, may not - **(i)** become, or continue as, an institution-affiliated party with respect to any insured depository institution; **(ii)** own or control, directly or indirectly, any insured depository institution; or **(iii)** otherwise participate, directly or indirectly, in the conduct of the affairs of any insured depository institution; …
> * * *

(b) Penalty

> Whoever knowingly violates subsection (a) of this section shall be fined not more than $1,000,000 for each day such prohibition is violated or imprisoned for not more than 5 years, or both.

If an employee is found to have committed a dishonest or fraudulent act, CCB is required by law to report the act, as soon as it is discovered, to the Federal Bureau of Investigation, the U.S. District Attorney, the bonding company, the Supervisor of Banking, and the Federal Deposit Insurance Corporation. In addition, Part 353 of the FDIC Rules and Regulations requires CCB to report suspicious activities to the Financial Crimes Enforcement network (FinCEN). Prohibited acts and activities, which may or may not trigger CCB's reporting obligations, include, but are not limited to:

- Theft
- Embezzlement
- Frauds such as forgery, counterfeiting and check kiting
- Insider abuse
- Misappropriation of, misapplication of or unauthorized use of funds, revenues, fees, or other property
- Abstraction or the wrongful taking or withdrawing of funds
- Deliberate misrouting of checks to delay payment
- Mis-posting accounts to favor oneself or another's account
- Arranging an otherwise legitimate loan, the proceeds of which were returned to the employee
- Unauthorized sale or disclosure of confidential information
- Any agreement to make or participation in making an impermissible "golden parachute payment" or indemnification payment in violation of Section 18(k) of the FDIA and Part 359 of the FDIC Rules and Regulations
- Any agreement to make or participation in making any employment contract, compensation or benefit agreement, fee arrangement, perquisite, stock option plan, post-employment benefit, or other compensatory arrangement that (i) would provide any executive officer, employee, director, or principal shareholder with excessive compensation, fees or benefits; or (2) could lead to material financial loss to the institution as further explained in Section 39(c) of the FDIA
- Abstracting, removing, mutilating, destroying, or secreting any paper, book, or record of CCB for the purpose of concealing any fact or suppressing any evidence against himself or herself, or against any other person
- False or inaccurate statements or entries or activities that result in such false or inaccurate statements or entries
- Making any other false entries, records, or reports

These acts are specifically cited in the U.S. Criminal Code, 18 U.S.C. § 1005: "Whoever, being an officer, director, agent or employee of any Federal Reserve Bank, member bank, depository institution holding company, national bank, insured bank … makes any false entry in any book, report, or statement of such bank … with intent to injure or defraud such bank … or any other company, body politic or corporate, or any individual person, or to deceive any officer of such bank, … or the Comptroller of the Currency, or the Federal Deposit Insurance Corporation, or any agent or examiner appointed to examine the affairs of such bank, … or the Board of Governors of the Federal Reserve system … shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both."

In addition, the U.S. Criminal Code, 18 U.S.C. § 656 provides: "Whoever, being an officer, director, agent or employee of, or connected in any capacity with any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, … embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of such bank, … or any moneys, funds, assets or securities entrusted to the custody or care of such bank, … or to the custody or care of any such agent, officer, director, employee or receiver, shall be fined not more than $1,000,000 or imprisoned not more than 30

years, or both; but if the amount embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both."

The U.S. Criminal Code, 18 U.S.C. § 643 provides: "Whoever, being an officer, employee or agent of the United States or of any department or agency thereof, having received public money which he is not authorized to retain as salary, pay, or emolument, fails to render his accounts for the same as provided by law is guilty of embezzlement, and shall be fined under this title or in a sum equal to the amount of the money embezzled, whichever is greater, or imprisoned not more than ten years, or both; but if the amount embezzled does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both."
While the statutes are directed to convicted dishonest acts in bank employment, non-employment convictions of dishonest acts would correspondingly be regarded as grounds for disciplinary action up to and including termination.

If you become aware of dishonest acts being committed toward CCB by other employees, officers, or directors, you must call such matters to the attention of either your immediate supervisor or the Human Resources department, who will inform the President and CEO. Failure to disclose known dishonest acts can classify a person as an accessory to the wrongdoing. The President and/or CEO shall immediately inform the Board of Directors of such action. If the dishonest act involves Human Resources or the President and/or CEO, contact Chris Adams, the audit committee chairman for the board of directors at chris.adams@adamslawyers.com or 425-387-0411.

In addition, any officer or employee who is charged with, or is entering into a pretrial diversion or similar program for any crime involving breach of trust, dishonesty, money laundering, a drug-related offense, a crime of violence or a felony must immediately notify the Corporation’s Chief Human Resource Officer.

INTEGRITY AND HONESTY

CCB expects its officers, directors, and employees to maintain the highest standards of integrity and ethical values. CCB presents its organization honestly to its officers, directors, and employees, and in turn, expects officers, directors, and employees to be honest in their dealings with CCB, its customers and fellow officers, directors, and employees. We expect people to be honest in their handling of money, merchandise, and property with which they are entrusted. Officers, directors, and employees are also expected to be honest with respect to the time, effort, and complete performance of their jobs as well as when dealing with others. In particular, officers, directors and employees are expected to respond honestly and candidly when dealing with CCB's independent and internal auditors, regulators and attorneys.

Approved by the Board 12/14/2022

ATTACHMENT B- INFORMATION SECURITY & TRAINING

The confidentiality and protection of customer information is one of the Bank's fundamental responsibilities. While information is critical to providing quality service, we recognize that our most important asset is the trust of our customers.

The Bank has established security and control measures to address the various risks to customer information and customer information systems. Risks include unauthorized access, fraud, negligence and destruction of data or property.

All persons who have access to corporate information will be required to understand and comply with all standards and procedures established. Every employee, to protect customer information and ensure the continuity of CCB business, will implement security measures.

Access to corporate information will be made available only to the extent necessary to support authorized business functions. The degree of information security protection is to be commensurate with the impact of inadvertent or intentional misuse, improper disclosure, damage, or loss. Information is classified into the following three categories:

- **Public** information comes from public sources or is provided by the company to the general public. Examples include periodicals, public bulletins, published company financial statements, published press releases, etc. Public information requires minimal security protection.

- **Restricted** information requires a level of security protection to ensure privacy and confidentiality. This is the kind of information most of us deal with on a day-to-day basis. Examples are customer/account information, financial records, correspondence, information about employees, passwords, etc.

- **Access** to restricted information should be controlled with protective measures that range widely, depending on the level of exposure. Protection measures include a "clean desk" with all documents and files put away, locks on building doors, office doors, desks, file cabinets, and computerized access controls for computer files, and disposal by shredding.

- **Confidential/Sensitive** information requires more extensive security protection because of potentially severe financial or competitive impact, or potential fraud. Examples are customer lists, information about pending acquisitions, PINs, dormant account information, data encryption keys, etc.

Access to confidential information should not only be controlled as with restricted information, but may also require special protection measures including special locked storage areas, secured off-site storage, "confidential" marking stamps, etc.

The ultimate responsibility for safeguarding Bank and customer information lies with each individual employee. Therefore, all employees who have access to systems that store and/or access such information are required to understand and comply with any and all specific policies, procedures, standards and guidelines established in support of the Information Security Program.

This Guide was created to assist the Bank employees in safeguarding the information assets of the Bank as well as the confidential information of our customers. The guide is not a replacement of Bank policy but acts as a companion to the various policies that affect how employees protect Bank information.

Comments regarding the Guide should be sent to the Bank's Information Security Officer.

Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), requires banks to maintain procedures that protect consumers' personal financial information. There are three principal parts to the privacy requirements: 1) Financial Privacy rule: 2) Safeguards (safeguarding of customer information) and 3) pretexting provisions.

The Financial Privacy Rule, also referred to as Regulation P, governs the collection and disclosure of customers' personal financial information. The Safeguards Rule requires the Bank to design, implement and maintain safeguards to protect customer information. The pretexting provisions protect information under false pretenses – a practice known as "pretexting" (pretexting is covered in the Social Engineering section of this guide).

Collection of Customer Information

Customer information is gathered from many different sources such as deposit accounts, loans, and other transactions with the Bank.

When a customer opens a deposit account, we collect information about the customer such as their name, address, tax identification number, telephone numbers, date of birth, mother's maiden name, driver's license number, credit report information, and their signature.

When a customer requests a loan, in addition to the information we would collect for a deposit account, we collect additional information related to employment, income, assets, existing liabilities, dependents, financial and credit history and any other relevant information.

During the course of handling a deposit account or a loan, the Bank collects transaction information about a customer such as balances, payee information, overdrafts, and non-sufficient funds, payment history, address changes and changes in credit or financial stating.

We also collect information from our customers when they send email correspondence through the Internet.

The Bank's Privacy Policy describes in detail how the Bank manages customer information and under what circumstances such information may be released to third parties. This policy is disclosed to Bank customers at the time a new account is established or upon request. As stated in our Privacy Disclosure, the Bank does not sell customer information, nor does it disclose any nonpublic personal information about customers to third parties except as permitted by law.

MAINTENANCE OF CUSTOMER INFORMATION

Customer information, whether on paper or electronic form, may be maintained when the Bank transmits or stores information.

Information is transmitted when it moves from one person or place to another. Examples of information transmission include but are not limited to:

- Written Correspondence
- E-mail
- Voicemail
- Information posted or submitted on or through the Internet or our other media

- Wires and ACH Transaction
- Intranet
- Fax Transmissions
- Telephone Conversations
- Business meetings
- Presentations
- Scratch paper, sticky notes
- Electronic Banking

The Bank stores information maintained for reference and future action. Examples of stored information include, but are not limited to:

- Servers and Network Storage
- Shared LAN (local area network) or WAN (wide area network)
- Statements and checks held in branch
- Signature Cards
- Loan Files
- Hard copies of reports
- All other paper containing customer information

Bank policy requires employees to lock or secure all customer documents. If an employee is leaving their workstation, they are required to lock their computer anytime they step away. When leaving your workstation, documents should be secured. When not returning for long periods, such as lunch, or leaving for the day, employees are required to lock or secure all customer documents.

Information recorded on documents, when no longer needed or required, should be placed in the shred bin. Shred bins are locked at all times. When the shred bins are serviced, an employee accompanies them during the shredding process. The shred company should never be left unattended during the shredding process.

IDENTITY THEFT

Identity theft is one of the fastest growing white-collar crimes in the U.S. Banks absorb most of the economic losses from credit and deposit account fraud associated with theft of consumer identities. The combination of these facts makes identity theft a significant issue for the Bank and a risk that every employee must be constantly aware of and continuously seeking to deter and detect.

Identity theft is the fraudulent use of an individual's personal identifying information. Often, identity thieves will use another individual's personal information such as name, social security number, driver's license number, mother's maiden name, date of birth or account number, to fraudulently open new credit card accounts, charge existing credit card accounts, write checks, open bank accounts or obtain new loans.

Identity thieves use various techniques to steal the information. The following are examples of the most common techniques:

- Impersonating victims in order to obtain information from banks and other businesses
- Stealing wallets that contain personal identification information and credit cards
- Stealing bank statements from the mail
- Diverting mail from its intended recipients by submitting a change of address form
- Rummaging through trash for personal data

- Stealing personal identification information from workplace records
- Intercepting or otherwise obtaining information transmitted electronically

Identity theft may go undetected for months and even years. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill.

TYPES OF IDENTITY THEFT

There are two basic types of identity theft: 1) account takeover; and 2) application fraud.

Account takeover occurs when an identity thief acquires a victim's existing account information and purchases products and services using either the actual credit card/check or the account number an expiration date.

Application fraud is what is referred to as "true name fraud." With application fraud, the thief uses the victim's social security number and other identifying information to open new accounts in the victim's name – but the phone and address information is usually changed to that which is controlled by the thief in order to prevent the victim from learning of the theft and to facilitate the receipt of fraudulent credit cards, etc.

Verifying Customer Identity

In order to reduce the risk of establishing fraudulent accounts or divulging confidential customer information to identity thieves, each Bank department that deals with customer information has developed specific verification procedures to guide employees in confirming the customer's identity before establishing a new account or releasing customer information. Bank procedures may involve a combination of positive, logical, and negative verification procedures.

Positive Verification

These procedures involve the comparison of information provided to information maintained by third parties (for new accounts) or Bank systems (existing customers). For example, an identity thief may provide the true name of an individual and a correct phone number, but an erroneous address. The bank could detect this discrepancy by checking the address information contained on a credit report (i.e., ChexSystems, Experian, Equifax, Trans Union or in the Bank's Customer information File. Another example includes contacting an applicant's employer. An identity thief may provide the name of a legitimate employer but may not provide the correct telephone number. Whenever contacting a reference, the Bank employee should not solely rely on the number provided but also use the phone book or the Internet white/yellow pages directory to independently verify the telephone number.

Logical Verification

These procedures assess the consistency of the information provided on an application. Logical verification may reveal inconsistencies in the information provided by an applicant. For example, the Bank can verify if the telephone area code provided on the application corresponds to the address provided or whether the customer lives/works near the branch. Inconsistent information does not automatically indicate fraud. For example, a customer may use a cell phone that is assigned to a different area code than the customer's home address. In such instances, the employee should inquire regarding the inconsistency to determine if the information provided appears reasonable.

Negative Verification

These procedures ensure that information provided on an application has not previously been associated with fraudulent activity. Reviewing credit reports for fraud indicators is a form of negative verification.

Assisting Victims of Identity Theft

The nationwide increase in identity theft crimes makes it likely that customer service employees will encounter Bank customers who have become victimized by identity thieves. If a customer requests assistance in resolving a case of identity theft, employees should provide the following information:

- Recommend that customers review account statements immediately and report any suspicious activity to the Bank
- Provide information about fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud
- Suggest that the customer file a police report to document the crime
- Recommend that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted
- Inform the customer that they may obtain a credit report free of charge (www.annualcreditreport.com)

Provide the customer information about the availability of the Federal Trade Commission's (FTC's) online guidance regarding steps a consumer may take to protect themselves against identity theft including the web address http://www.ftc.gov/bcp/edu/microsites/idtheft and the toll free number (877) IDTHEFT {(877) 438-4338} that consumer may use to obtain ID theft guidance.

Social Engineering

Social engineering is the attempt to manipulate or trick a person into providing confidential information to an individual that is not authorized to receive such information. In banking there are four common types of social engineering techniques: 1) pretext calling; 2) dumpster diving: 3) shoulder surfing; and 4) identity theft. This section will cover the first three. Identity theft was covered in the prior section.

Pretext Calling

Pretext calling is a fraudulent means of obtaining an individual's personal information. Armed with limited information, such as a customer's name, address and/or social security number, a pretext caller may pose as a customer or an employee in an attempt to convince a Bank employee to divulge confidential information.

Information obtained through pretext calling may be sold to debt collection services, attorneys, and private investigators for use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts. In some instances, pretext callers may call an institution repeatedly until the caller finds an employee willing to provide the information.

Pretext calling is difficult to detect. While information brokers and private investigators routinely advertise their ability to locate and provide specific information about individual bank accounts, banks and their customers are likely to be unaware that they have been victims of "pretexting" (i.e., the use of some form of pretext to obtain customer information). Unless the pretexting ultimately leads to identity theft, it may go undetected altogether.

Each department within the Bank that deals with customers and customer information has implemented specific procedures to protect customer information from being inappropriately released to third parties. Each employee is responsible for understanding and complying with Bank and department – specific procedures regarding Customer Identification. (CIP)

The list below identifies potential pretext caller situation. While calls that resemble these examples are not necessarily pretext calls, extra care should be taken to ensure the authenticity of the call:

- A caller who cannot provide all relevant information
- An employee caller that cannot provide basic security information that is readily available to all employees
- An employee caller whose Caller ID does not agree with that employee's location
- A caller who is abusive and attempts to get information through intimidation
- A caller who tries to distract the Bank employee by being overly friendly or engaging the employee in unrelated "chit-chat" in an effort to change the employee's focus
- Any caller who appears to be trying to get the employee to circumvent Bank policy through some tactic that is intended to persuade the employee

Pretext callers may "nibble" Bank employees until they build a complete customer profile. Callers may also nibble for information about Bank employees. Nibbling refers to calling and obtaining what appears to be small, insignificant information. However, through nibbling, the pretext caller places multiple calls to different Bank locations, each time collecting an additional piece of information. After numerous successful attempts, the pretext caller has obtained sufficient information to create a complete profile. As such, employees need to treat all information as highly sensitive and confidential.

Dumpster Diving

Dumpster diving is a common technique used by identity thieves to obtain confidential information. Dumpster diving involves rummaging through a company's trash to collect customer information. Identity thieves can rummage through office trashcans or through large dumpsters. Either way, the objective is to gather information that has been carelessly thrown away.

Branch personnel should periodically empty the trash receptacles near the check-writing counter. Many customers discard account information in the receptacle that could be taken and used inappropriately. The Bank has implemented the following procedures to prevent the use of dumpster diving:

- **Shred Bins**: Any documents that contain confidential company or customer information must be discarded into one of the many shred bins located throughout the Bank. The use of shred bins ensures that confidential documents are not discarded with the Bank's usual trash and as such are not susceptible to dumpster diving attempts. These shred bins are emptied, and the contents shredded at our locations by a bonded operator who provides this service.

- **Paper Shredders**: Some offices are equipped with personal paper shredders to provide immediate shredding of sensitive documents.

Shoulder Surfing

Procedures that prevent identity theft and ensure adequate protection of confidential information extend beyond pretext calling and dumpster diving. Adequate security procedures also require employees to protect against "shoulder surfers."

Shoulder surfers are criminals that acquire personal information through eavesdropping. Shoulder surfers may obtain information while standing in line at the Bank branch or ATM. Others may use binoculars to spy on their victims. Still others may stand outside branch windows and observe computer screens that contain confidential account information. In all instances, the objective is to obtain confidential information.

The risk of shoulder surfing requires all employees to be aware of their surroundings when working with confidential information. The following are some steps that should be taken by Bank employees to ensure protection from shoulder surfers:

- Ensure that computer monitors are positioned in a manner that prevents individuals from observing confidential information (i.e., do not place computer screens in plain view of windows or spaces accessible by the public). If this is not feasible then the employee should request a protective screen that is placed on the monitor to prevent others from easily viewing the contents of the computer screen. When unattended, make sure computer screens are turned off or a screen saver has been engaged.
- When in a face-to-face situation with a customer, ensure that the sharing of confidential information is provided in writing. To prevent someone from learning the information through eavesdropping, do not request that the customer provide such information verbally. The same practice applies when the employee provides the customer with confidential information. Remember to properly dispose of such information after it has been provided; and,
- Ensure that adequate space exists between the customer conducting transactions and other customers standing in line. Proper spacing will enhance customer privacy and deter criminals from acquiring confidential information such as PIN, account number, balance, etc.

PASSWORDS

Passwords are unique strings of characters that employees provide in conjunction with a user ID, to gain access to an information resource. Passwords are an important aspect of information security because they are the first line of defense in protecting Bank and customer information. Passwords should be strong and unique to each site. A poorly chosen password may result in the compromise of confidential information that could adversely affect both the Bank and its customers.

All employees are responsible for taking the appropriate steps to select and secure their passwords. This section establishes best practices for password selection as well as protection and use of passwords. CCB provides employees with access to secret server password manager to help keep complex passwords secure.

General Password Guidelines

Bank employees use passwords to access various resources. These resources include access to personal computers, voicemail, the core, and other processing applications, etc. User IDs and passwords are used to authenticate employees to the particular resource and are used to track user activity while using that resource. Temporary passwords are usually assigned to employees when access is initially granted to a resource. Employees are forced to change their passwords upon initial log on. It then becomes the employee's responsibility to establish a strong secure password.

Employees must be aware of the characteristics of strong and weak passwords in order to ensure adequate protection of Bank and customer information. If someone obtains an employee's User ID and password, that individual can imitate the employee without the system knowing. Any damage created by the intruder will appear to have been created by the employee.

Poor, weak passwords have the following characteristics:

- Password contains less than eight (8) characters
- The password is a word found in the dictionary
- Password is names of family, pets, friends, co-workers, sports teams, movies, shows, license plate number, birthdates, etc.
- Password is computer terms and names, commands, sites, companies, hardware, software

- The words “password,” “CCB,” etc. are included

Strong Passwords have the following characteristics:

- Contain mix of letters, both upper and lower case
- Use numbers and symbols, along with letters
- Are at least 15 characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Employees should never write down the password or passphrase. Instead, employees should create passwords that can be easily remembered. One way to accomplish this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be “every day I read the green book with my favorite pet and the password could be “ED1rGb@@kwmfP3T” or some other variation. CCB provides employees with access to secret server password manager to help keep complex passwords secure.

Password Protection

Refrain from using the same password for Bank accounts as for other non-Bank accounts (i.e., personal email account, etc.). When possible, refrain from using the same password for multiple Bank accounts. For example, use a different password for the Network and other applications (Horizon, ImageCentre, etc.). Do not share passwords with anyone, including Bank personnel. All passwords must be treated as highly sensitive information.

The following is a list of things that employees should NOT do:

- Don’t reveal your password over the phone to anyone – not even individuals who claim to be calling from the IT department
- Don’t reveal your password in an email message
- Don’t reveal your password to your manager or any other Bank employee.
- Don’t talk about your password in front of others.
- Don’t hint at the format of a password (i.e., my family name)
- Don’t reveal your password on questionnaires or security forms
- Don’t share your password with family members
- Don’t reveal your password to co-workers while on vacation
- Don’t leave your password anywhere on or near your workstation (i.e., post –it-notes, under mouse pads, etc.)
- Don’t create passwords for group use or shared passwords. Passwords should be unique to each person.

Do not provide your password to anyone who requests or demands it. Refer the incident to the Bank’s Information Security Officer. Immediately change your password if you suspect that your password has been compromised.

Changing Passwords

Bank policy requires passwords be changed regularly, but an employee may change a password at any time if there is a possibility that the password has been compromised. Generally, the Bank’s various computer systems do not permit employees to reuse a previously used password for a minimum period of time, as defined by the system. Systems prompt for password changes when change is required. To save time and effort, passwords should be changed before they expire.

For more information regarding the Bank's password standards refer to the Bank's Employee Handbook or contact the Bank's Information Security Officer or IT Manager.

EMAIL

The Bank grants email capabilities to employees in order to provide an efficient manner of communication among Bank employees and individuals outside the Bank. If used appropriately, email has the potential to offer the following benefits to Bank employees:

- Encouragement of teamwork – particularly among individuals who are geographically dispersed
- Cost-effective and environmentally friendly means of day-to-day communication
- Ability to disseminate information in a timely manner
- Rapid delivery of administrative information to Bank personnel

The use of email also creates risks to the Bank that must be properly managed to ensure adequate protection of Bank assets as well as customer information. Risks created through the use of email include:

- Inadequate awareness among email users regarding the fact the email is not a secure form of communication, and that privacy and confidentiality are not guaranteed by the Bank.

Delivery of inappropriate material to and from Bank email accounts

- Problems related to information overload when large quantities of information, some of marginal value, are delivered to individuals' email accounts
- Difficulty in controlling record keeping and legal liability issues

Expectation of Privacy

While employees are provided with email accounts that are protected by the Network login password, it is not intended to assure employees that email communications will be kept confidential. The Bank maintains the right to access any employee's email communications and to retrieve stored email information.

Appropriate Use

Email capabilities are provided strictly for business purposes. Emails sent and received by Bank employees are considered Bank property. The use of email via the Bank's facilities and/or equipment, by an employee, constitutes acknowledgment and understanding that the employee is representing the Bank. Incidental and occasional personal use of email is permitted. However, such use will not be confidential and must comply with this section of the Guide as well as any other Bank policies covering such use. Further, any incidental email usage may not interfere with the employee's official duties and must have a minimal effect on the Bank.

General Guidelines

- The email system should not be used to communicate confidential Bank or customer information to anyone outside the Bank.
- Bank employees are prohibited from reading email communications delivered to another Bank employee's mailbox without proper authorization from the Bank's VP of IT or Information Security Officer. Further, any employee who received an email communication intended for someone else must immediately inform the sender that the email communication was sent to the wrong person. The employee must delete the email communication.
- The email system must not be used for any form of harassment, threat or any communication that could be deemed abusive, defamatory, obscene, offensive, derogatory, or otherwise inappropriate, illegal, or unrelated to Bank business. This includes a prohibition against email communications that harass or offend on the basis of race, color, religious belief, sex, sexual orientation, national origin, ancestry, age, marital status, disability, mental condition or veteran status.

- Employees may not use the email system for the purpose of personal or no-Bank solicitations (i.e., spam, etc.). Examples include but are not limited to anything in conjunction with an employee's outside business endeavors or sales of any product or outside service (i.e. home products, cosmetics, etc.).
- Employees may not use the email system to deliver messages related to political issues (i.e., encouraging or advocating a certain position, bill, etc.).
- Messages that violate Bank policy or that are contrary to supervisory instructions are not permitted.
- Personal announcements (i.e., items for sale, requests for roommates, etc.) are not acceptable.
- The email system may not be used to create or forward "chain letters," "Ponzi" or "pyramid" schemes of any type.
- Employees must avoid opening email attachments received from unknown senders, which may contain viruses or other malicious computer programs.
- Emails to "All Bank Employees" should be well conceived and should be reviewed by a supervisor prior to sending.
- If at any time you receive an email that you believe may be fraudulent, you should delete the email. Never click on a link within an email that was unsolicited or not expected.
- Employees should not forward Bank emails to their personal email address.

Security

Email messages that are sent outside of the Bank are **not** secure, unless sent by typing 'secure:' in the subject line before adding the subject or using ShareFile.

Risks to email include someone intercepting the message during transit or the message being inadvertently delivered to the wrong person. Another risk is someone forwarding a private/confidential email to someone else. These risks are increased when the email is accessed/delivered through the use of Webmail.

As such, employees should never include anything in an email message that is private or confidential or that could create the risk of litigation or otherwise put the Bank at risk, unless sending secured. To obtain more information on sending a secure email, contact the Information Security Officer or VP of IT prior to sending an email.

The following are some examples of information that should not be included in an email:

- Passwords
- Confidential Bank or customer information (when delivering an email to an external party)
- Company secrets such as trade secrets, contracts, strategic plans, etc. (when delivering an email to an external party)

Legal Implications

Email is a formal means of business communication. Erasing an email does not necessarily erase all copies of the email. Archived copies of the email may reside for substantial periods of time, in the Bank's records. Archived copies of emails are subject to the same right to access as messages stored in an employee's mailbox. For these reasons, employees should refrain from including in an email anything they would not ordinarily include in a memorandum or state in the open or in a court of law.

Employees must be aware that email is subject to the full range of state and federal laws and regulations that apply to other forms of communication. Applicable laws and regulations affect issues such as copyrights, anti-discrimination, defamation, privacy, harassment, etc.

The ease of use and ability to conveniently contact a larger group of individuals makes it possible to inadvertently break the law or breach security and privacy. Through the use of law, regulation or agreement, certain third parties including attorneys and government agencies, may require the Bank to grant them access to stored email.

SECURITY BREACH

The following are some examples of security breaches:

- A person gains access to a computer on our network and is able to obtain the "personal information" of a Bank customer
- A file cabinet containing "personal information" appears to have been broken into and the contents appear to have been removed
- Employee emails a file containing "personal information" to an individual outside the Bank for purposes other than official Bank business
- Employee takes home and subsequently loses a CD-ROM or DVD containing customer loan information
- Employee loses a laptop containing customer loan write-ups and other loan application information
- Employee copies customer's personal information and uses information for unauthorized purposes
- Employee emails confidential/sensitive/customer information to employee's personal email address

Risks

Noncompliance with the Privacy Law can result in litigation risk in the form of civil damages, compliance consequences and/or lawsuits against the Bank. Another significant risk to the Bank is the reputation risk. A breach of personal information can create significant public relations challenges and the potential for the loss of customers.

Bank procedures

The most effective means of complying with the Privacy Law is to prevent the breach of any customer information. Breaches are prevented by exercising due care when working with customer data or computer systems that access such data.

Examples of due care includes:

- Logging off of the network when leaving a computer workstation for an extended period of time
- Protecting documents (reports – deposit slips – files- proof work) in your work area from inadvertent viewing by unauthorized persons. Observe the Clean Desk policy
- Empty daytime shred receptacles into the shred bin before you leave for the night
- Using password protected screensavers (i.e., locking your computer) when you leave your workstation. (Workstations are set to automatically lock after 10 minutes of inactivity)
- Refraining from copying customers' personal information
- Keeping items that contain personal information in a secure location
- Never emailing outside of the Bank any documents/files that contain confidential information
- Speaking softly when discussing sensitive information with a customer at your workstation. Be aware of standers by
- Ensure your workstation is positioned in a manner that prevents someone from viewing confidential information
- Do not allow remote access to your workstation, unless approved by IT
- External devices, such as USBs, are not allowed to connect to your workstation
- Protecting passwords

- Being alert to suspicious activity related to the theft/compromise of personal information

In the event an employee discovers a breach of customer information, the employee should immediately contact his/her manager. The manager will contact the Bank's Information Security

Officer will immediately assemble the Incident Response Team. The Information Security Program contains contact information and guidance to promptly choose the appropriate response.

Information Security Training Program

The Graham Bliley Leach Act (GLB) is a law that requires banks to ensure the confidentiality of customer non-public information.

It is the responsibility of every Bank employee, officer, and Director to be familiar with the Act and with the procedures in place that protect the privacy of customer information.

It is the responsibility of every Bank employee, officer, and Director to safeguard all customer non-public information by following the procedures in this program and all other related banking procedures.

Receipt of this training material and acknowledgment constitutes a commitment to read and understand the material. Any questions about the program or the GLB Act can be directed either to one's supervisor or the Information Security Officer of the Bank.

Approved by the Board 12/14/2022

ATTACHMENT C- PRIVACY SECURITY

PRIVACY OF CONSUMER FINANCIAL INFORMATION (REGULATION P)

CCB's mission is to provide locally owned business owners and community minded families with financial services including money management, commercial, and personal loans. We understand the needs of our communities and offer convenient access throughout the North Puget Sound.

As financial service providers, CCB is entrusted with sensitive financial information; we respect the privacy of our customers and are committed to treating customer information responsibly. Our Customer Information privacy policy serves as a standard for all CCB employees for collection, use, retention, and security of individual customer information.

Consumer Privacy Disclosure

CCB will provide a clear and conspicuous notice that accurately reflects the privacy policies and practices as they relate to: a) the bank's customers and b) consumers who may inquire or apply for the bank's services but do not become customers. This Privacy Notice will be given to the individual when that individual enters into a continuing relationship with CCB and then once annually during the customer relationship.

The Privacy notice will inform the customer of the following information:

- Categories of nonpublic personal information the bank collects
- Categories of nonpublic personal information the bank discloses
- Categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information
- Categories of nonpublic personal information about the bank's former customers that the bank discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about the bank's former customers
- An explanation of the consumer's right to opt-out of the disclosure of nonpublic personal information to nonaffiliated third parties and the ability to opt-out of disclosures of information among affiliates.
- The bank's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information
- Any exceptions to the opt-out requirements

CCB does not disclose nonpublic personal information about customers to anyone, except as permitted by law. When customers close accounts or become inactive customers, we adhere to the privacy policies and practices as described in our privacy disclosures. It is our policy not to reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except as permitted by law.

Confidentiality and Security

CCB is committed to the security of customer financial and personal information. All of our operational and data processing systems are in a secure environment that protects account information from being accessed by third parties. We maintain and grant access to customer information only in accordance with our internal security standards.

At CCB, employee access to personally identifiable customer information is limited to those with a business reason to know such information. Employees are educated on the importance of maintaining the confidentiality of customer information and on these privacy principles. Because of the importance of these issues, all CCB employees are responsible for maintaining the confidentiality of customer information and employees who violate these privacy policies will be subject to disciplinary measures.

Maintenance of Accurate Information

We continually strive to maintain complete and accurate information about customer accounts.

Maintaining Customer Privacy in Third Party Relationships

When CCB conducts business with third parties, we require vendors and suppliers to maintain similar standards of conduct regarding the privacy of personally identifiable customer information provided to them.

To Better Serve Internet Banking Customers

CCB collects generic information about visitors to our website. This information includes the date and time of access, the Internet service provider's address, the web browser used, and the visitor's physical location.

CCB requires customers to utilize specific passwords for access to confidential and private information. CCB reminds customers of their responsibility to safeguard login IDs and passwords. In addition, commercial customers are encouraged to carefully screen those employees to whom user IDs and passwords are granted.

CCB utilizes encryption, firewall, router, third party verification procedures and other security software and hardware to help prevent unauthorized eavesdropping of and access to customers' confidential and private information. This protects only the Bank's systems. Customers are encouraged to utilize security protection software on their own computers to protect their system from unauthorized access.

CCB utilizes virus protection software to help prevent the spread of computer viruses. This protects only the Bank's systems. Customers are encouraged to utilize virus protection software on their own computers to protect their systems from viruses.

CCB's cash management services and our website utilize "cookies" to help authenticate our customers' identities and to help facilitate the exchange of information between CCB systems and our customers' systems.

CCB reminds all of our customers that links on CCB's website can be found to websites not under our control. These websites will not necessarily comply with CCB's Privacy Principles and security standards.

CCB reminds all of our customers that confidential and private information may be compromised in both traditional and non-traditional banking activities. CCB can only establish procedures to help restrict use of and access to confidential and private information. If any CCB customers believe that confidential and private information has been compromised, they are encouraged to contact CCB immediately so that the potential breach can be investigated.

Security / Privacy Procedure
Request for Customer Information

CCB has policies in place for protecting customer information. It is the responsibility of each employee to take every precaution in discussing any information regarding our bank customers.

When you have a customer asking you for information on their accounts with us, you must always treat them with courtesy and respect.

Prior to releasing any information:

- You must identify the customer.
- Verify either with the signature card or on the relationship screen on *Horizon* that they are authorized to receive information on the account. Remember, only authorized signers, or in special cases, individuals that we have written authorization allowing "inquiry" access, can be given any information on an account.
- Someone having access to one account does not give them authorization to access information on similar accounts. Example: Husband and wife have a joint account with the bank. Both parties are authorized to receive information on the joint account. If the ·wife also has an Individual account with the bank; the husband does not have the authority to access any information on her personal account.
- Information needs to be given to the customer in a confidential manner. Balances should be given in writing, not verbally.
- If a request requires a more involved explanation, it is preferred that the customer be assisted at a desk away from other customer activity.
- If someone comes in to make deposits to a customer's account other than their own account, they need to provide a completed deposit slip that includes the account number. One tactic that is used to locate where someone banks is to go into different banks claiming you want to make a deposit to "Joe Smith's" account, but don't have the account number. If the bank provides that information, we have just given out confidential information about our customer. Even if you don't give out the actual number, you have confirmed that "Joe Smith" does indeed bank with us.

If you feel uncomfortable or are unsure of any request for information, it is always advisable to refer the request to your manager

Written or Faxed Requests for Information

The bank Operations department should handle all written or faxed requests for customer information. This allows for a consistent review of the requests received, and a central file for maintaining our response to all written inquiries.

If you receive a written request for information, please date stamp the request and forward it to bank operations.

- Operations will validate the customer's signed authorization form using customer signature cards and, in some cases, calling the customer to obtain a verbal confirmation of the written request to release information.
- Copies of the request and our response will be maintained either in the Correspondence file or the Verification file in the Operations department.
- Response to legal requests for information will-be maintained in an appropriate legal file. Examples: Subpoenas, Levy, and Garnishments.
- No information will be released based on verbal requests from law enforcement or for any other legal purpose. The bank must have a Subpoena or legal document requesting the information.

Call Operations Department with any questions regarding written requests for information

Telephone requests for Information

It is not advisable to discuss customer information over the phone. You must be certain you are able to identify the caller. When responding to telephone requests for information, our primary responsibility is

to protect the privacy of our customers. Pretext calling is a scam used to gain access to confidential customer information. The pretext caller may have· some basic information on our customer: name, address, and social security number. They will often have account numbers, and be looking for balance information, or other specific account information.

If you do not recognize the caller's voice, use the following guidelines to establish their identity:

- Let the customer know the reason you are asking all of the questions. "I'm sorry, I don't recognize your voice over the phone. We don't normally give out customer information on the phone. I need to ask these questions to protect your privacy."
- The caller must have the account number. We will not give out account numbers over the phone.
- Ask for the basic information first. Name, account number and social security number. Once you have the account information open on the Core system, ask for further information to identify the customer.
    - Mother's maiden name
    - Date and amount of last deposit
    - Account opening date
    - Check number and amount of last check written.

If you are not positive, ask the customer if they are calling from their home phone or work phone. Using the number listed on the Core system, you can call the customer to relay whatever information they have requested. *(You can see the importance of getting accurate information when opening an account)*.

Inform the customer of the access available using our 24-hour telephone banking system at 1-800-958-2382 or local 425-252-7822 or Online Banking.

PRIVACY AWARENESS TIPS FOR EMPLOYEES

- **Log Off-** Don't leave sensitive customer information on your desk or computer screen unattended. Log off the system if you need to leave your desk or teller window.
- **Shred**-Foil "dumpster divers'' by shredding any documents such as account statements and applications- before discarding them.
- **Securely Store**-Keep all documents and reports safe by locking file cabinets.
- **Put Away** Documents-When you are finished helping one customer, put away any documents containing that customer's personal information before helping the next customer.
- **Authenticate-**Never give customer information over the phone unless you have initiated the call or have followed the appropriate identification procedures.
- **Follow Procedures**-Always follow the procedures "'Request for Customer Information''.
- **Scrutinize-**Carefully scrutinize all requests for account information or requests to change account information, i.e., address change, name change.
- **Resist Intimidation**-Don't be intimidated by requests for information from someone claiming to be with the government or a law enforcement agency. We are not required to provide such information without a subpoena.
- **Report Suspicious Activity**-Report any suspicious requests for customer information to the Security officer.

Spotting and Avoiding Pretext Calls

We need to be aware of the use of pretext calls by information brokers and identity thieves to gain unauthorized and often illegal access to customer information.

Private Investigators and collection agencies have been traditional users of pretext calls to gain access to customer information. Keep in-mind that they have birth date, social security number and in some case's their mothers' maiden name.

In most pretext calls, the caller will be missing one or more pieces of information that the customer should know to identify themselves. The most common missing pieces of information are, account number, mother's maiden name, amount or date of last deposit or withdrawal, the address of the institution where the account was opened, or the date when the account was opened.

Signs of a possible pre-text call:

- Missing Important Account information
- Callers who are hesitant or refuse to give a call back number
- Out of the ordinary request
- Overly aggressive callers
- Overly Talkative callers
- Absentminded callers

It is our responsibility to first determine what individuals and/or entities are currently granted access to customer information and under what circumstances.

Customer Research/Response Resolution

All customer complaints and requests for resolution will be filed in a centralized location with the Compliance Officer. All complaints are to be immediately forwarded to the Compliance Officer; see your supervisor for instructions.

All customer requests will be directed to the Operations Department. It may be assigned to another staff member after review by one of these individuals.

Customers should be contacted within 48 hours acknowledging receipt of the complaint/inquiry.
It may not be possible to resolve disputes within that time frame; however, every attempt will be made to resolve the customer complaint.

Approved by the Board 12/14/2022

ATTACHMENT D- INSIDER TRADING POLICY

Coastal Community Financial Corporation (the "Company") is a public company, the common stock of which is traded on the Nasdaq Global Select Market and registered under the Securities and Exchange Act of 1934, as amended. As a public company, the Company files periodic reports and proxy statements with the Securities and Exchange Commission ("SEC"). Investment by directors, officers and employees in Company common stock is generally desirable and encouraged. However, such investments should be made with caution and with recognition of the legal prohibitions against the use of confidential information by "insiders" for their own profit.

As a director, officer, or employee of a public company or one of its subsidiaries, you have the responsibility not to participate in the market for Company common Stock while in possession of material, inside information about the Company. There are harsh civil and criminal penalties if you wrongly obtain or use such material, inside information when you are deciding whether to buy or sell securities, or if you give that information to another person who uses it in buying or selling securities. If you buy or sell securities while in possession of material, inside information, you will not only have to pay back any profit you made, but you could be found guilty of criminal charges, and face substantial fines or even prison. Additionally, the Company could be held liable for your violations of insider trading laws.

In order to avoid these harsh consequences, the Company has developed the following guidelines to briefly explain the insider trading laws and set forth procedures and limitations on trading by directors, officers and employees. However, these guidelines do not address all possible situations that you may face. In addition, you need to review and understand the Company's Policy on Fair Disclosure to Investors that describes your obligations regarding the selective disclosure of confidential information to ensure compliance with SEC Regulation FD, which requires "fair disclosure" of material, non-public information.

Insider Trading Concepts

What is "Inside" Information?

Inside information includes anything you become aware of because of your "special relationship" with the Company as a director, officer, or employee and which has not been disclosed to the public (*i.e.*, is non-public). The information may be about the Company, any of its subsidiaries, or other affiliates. It may also include information you learn about another company, for example, companies that are current or prospective customers or suppliers to the Company or those with which the Company may be in negotiations regarding a potential transaction.

What is Material Information?

Information is material if an investor would think that it is important in deciding whether to buy, sell or hold stock, or if it could affect the market price of the stock. Either good or bad information may be material. If you are unsure whether the information is material, assume it is material.

Examples of material information typically include, but are not limited to:

- financial or accounting problems.
- estimates of future earnings or losses.
- events that could result in restating financial information.
- a proposed acquisition, sale, or merger.
- changes in key management personnel.
- beginning or settling a major lawsuit.
- changes in dividend policies.

- declaring a stock split.
- a stock repurchase program; or
- a stock or bond offering.

What is Non-Public Information?

Non-public information is information that has not yet been made public by the Company. Information only becomes public when the Company makes an official announcement (in a publicly accessible conference call, a press release or in SEC filings, for example) and people have had an opportunity to see or hear it.

Trading Guidelines

A. Rules applicable to all directors, officers, and employees.

No director, officer or employee may trade *any security*, whether issued by the Company or by any other company, while in possession of "material inside information" about the issuer. Further, no director, officer or employee may disclose "material inside information" to any other person (including immediate family members, friends, or stockbrokers). It is usually safe to buy or sell stock after the information is publicly announced, if you do not know of other material information that has not yet been announced. Even after the information is announced, you should wait at least two full trading days before buying or selling securities to allow the market to absorb the information.

This means the following with respect specifically to certain Company employee benefit plans:

- 401(k) Plan. An officer or employee having material inside information regarding the Company may not initiate a transfer of funds out of the Company stock fund of the 401(k) plan.
- Other Company stock purchase plans. A director, officer or employee having material inside information regarding the Company may not sign up for, or increase/decrease participation in, any employee stock purchase plan or dividend reinvestment plan. However, ongoing purchases through those plans pursuant to a prior election are not prohibited.
- Stock Options. A director, officer or employee may exercise a stock option at any time, but any stock acquired upon such exercise may not be sold (whether by means of a cashless exercise or otherwise) if the individual has material inside information regarding the Company. At any time, however, an individual may deliver Company stock already owned to pay the option exercise price and taxes.

B. Additional rules applicable to all officers with the title of Senior Vice President or higher, all directors, and all persons in the Accounting Department and the Treasury Department, all persons who work within the Executive Offices of the main office and such other employees as may be designated by the President and Chief Executive Officer as members of the Restricted Group (the "Restricted Group").

1. **Blackout Periods**

Quarterly blackout periods. No person in the Restricted Group may trade in Company securities during a blackout period **that begins on the fifteenth day of the last month of each calendar quarter (*i.e.,* on December 15, March 15, June 15, and September 15)** and ends two trading days after the public release of the Company's earnings for such quarter. The blackout period applies to (i) open market purchases or sales, (ii) a sale of securities following exercise of a stock option (including a sale by way of a cashless exercise), (iii) signing up for, or increasing/decreasing participation in, any employee stock purchase plan or dividend

reinvestment plan, and (iv) initiating a transfer of funds into or out of the Company stock fund of the 401(k) plan or increasing an existing election to invest funds in the Company stock fund. However, ongoing purchases by any person through the 401(k) plan or other Company-sponsored plan pursuant to a prior election are permitted at any time, (*i.e.,* they are not subject to the blackout period). The Company's President and Chief Executive Officer, in consultation with Company counsel, may permit transactions during the blackout period upon request where the person making the request is not in possession of material inside information.

Temporary blackout periods. The Company may also institute temporary blackout periods in the event of a material corporate development. Notice of temporary blackout periods will be distributed by means of a written or electronic communication specifying the duration of the blackout period and the persons subject to it.

Written Plan. The limitations of the blackout periods shall not apply to trading in Company securities pursuant to a "written plan for trading securities" provided that such plan meets the requirements of SEC Rule 10b5-1 and is approved in advance by the Company's Board of Directors. See Section C.4.

2. **Selling short**. No person in the Restricted Group may at any time sell short Company stock or otherwise sell any equity securities of the Company that they do not own. Generally, a short sale means any transaction whereby one may benefit from a decline in the Company's stock price.

3. **Options.** No person in the Restricted Group may at any time buy or sell options on Company securities (so called "puts" and "calls") except in accordance with a program approved by the Company Board of Directors or a trade cleared by the President and Chief Executive Officer. This restriction does not apply to the exercise of employee or director stock options, which is treated under Section A above.

4. **Margin Accounts and Pledges**. Securities held in a margin account may be sold by the broker without the customer's consent if the customer fails to meet a margin call. Similarly, securities held in an account which may be borrowed against or are otherwise pledged (or hypothecated) as collateral for a loan may be sold in foreclosure if the borrower defaults on the loan. A margin sale or foreclosure sale may occur at a time when the pledgor is aware of material non-public information or otherwise is not permitted to trade in Company securities and, as a result, the pledgor may be subject to liability under insider trading laws.

   Therefore, you may not purchase Company securities on margin, or borrow against any account in which Company securities are held, or pledge Company securities as collateral for any loan.

   An exception to this prohibition may be granted where a person wishes to pledge Company securities as collateral for a loan from a third party (not including margin debt) and clearly demonstrates the financial capacity to repay the loan without resort to the pledged securities. Any person who wishes to pledge Company securities as collateral for a loan from a third party must submit a request for approval to the Company's President and Chief Executive Officer at least two weeks prior to the execution of the documents evidencing the proposed pledge.

C. Additional rules for Section 16 reporting persons.

1. **Pre-clearance and reporting:** Any trade of Company securities by a director or executive officer, or a family member sharing the same household or a corporation or trust they control, must be pre-cleared with the Filing Coordinator identified in the Company's Section 16 Compliance Program and must be reported promptly to the Filing Coordinator once made. **If,**

upon requesting clearance, you are advised that Company stock may not be traded, you may not engage in any trade of any type under any circumstances, nor may you inform anyone of the restriction. You may reapply for pre-clearance at a later date when trading restrictions may no longer be applicable. It is critical that you obtain pre-clearance of any trading to prevent both inadvertent Section 16(b) or insider trading violations and to avoid *even the appearance* of an improper transaction (which could result, for example, when an officer engages in a trade while unaware of a pending major development).

2. **Options and other stock plans**. The exercise of Company stock options and/or the sale of stock acquired upon an exercise, the transfer of funds out of the Company stock fund in the 401(k) plan, and other transactions in the Company's stock plans are subject to special rules. The Filing Coordinator must be contacted before any such transaction is conducted.

3. **Pension Fund Blackouts.** The Sarbanes-Oxley Act of 2002 also requires the Company to absolutely prohibit all purchases, sales, or transfers of Company securities by directors and executive officers during a pension fund blackout period. A pension fund blackout period exists whenever 50% or more of the plan participants are unable to conduct transactions in their accounts for more than three consecutive days. These blackout periods typically occur when there is a change in the retirement plan's trustee, record keeper or investment manager. Directors and executive officers will be contacted when these or other restricted trading periods are instituted.

4. **Pre-Clearance Policy for Rule 10b5-1 Plans.** Directors and executive officers may not implement a trading plan under SEC Rule 10b5-1 at any time without prior clearance. Directors and executive officers may only enter into a trading plan when they are not in possession of material inside information. In addition, Directors and executive officers may not enter into a trading plan during a quarterly blackout period or during a pension fund blackout period, if applicable. Once a trading plan is pre-cleared, trades made pursuant to the plan will not require additional pre-clearance, **but only if the plan specifies the dates, prices, and amounts of the contemplated trades or establishes a formula for determining dates, prices, and amounts.** Transactions made under a trading plan need to be promptly reported to the Filing Coordinator who will prepare the necessary SEC Form 4.

D. Additional rules applicable to proposed acquisitions.

Whenever the Company is actively considering a particular company for acquisition or for another significant business relationship (such as a joint venture) or whenever another company is considering acquiring the Company, all Company employees involved in, or aware of, due diligence or other planning for or attention to the acquisition or business relationship are prohibited from trading in any securities of the Company and any securities of the other company.

Note: This policy applies to personal securities transactions by the directors, officers and employees identified above and also applies to:

(a) transactions for accounts in which the Company director, officer or employee has an interest or an ability to influence transactions; and

(b) transactions by the director's, officer's or employee's spouse or any other member of their household unless (i) the household member's investment decisions are made independently of the Company director, officer, or employee and (ii) the household member has not received inside information about the issuer of the security. It must be understood, however, that the director, officer, and employee and/or the household member will bear the burden of demonstrating that the household member has not received inside information. **Furthermore, directors and executive officers are subject to special rules in this regard and any proposed transaction in Company securities by a corporation or trust they control or by**

a family member sharing the same household must be discussed in advance with the President and Chief Executive Officer or Company legal counsel.

Stock Repurchases by the Company.

The Board of Directors may delegate to the President and Chief Executive Officer or his designee(s) the authority and discretion to authorize the Company to purchase Company common stock pursuant to a Board-approved and currently effective stock repurchase program, including during a restricted trading period under this policy, provided that the President and Chief Executive Officer determines that the following conditions are met:

(a) the Company is not in possession of non-public material information that prohibits such purchases.
(b) market conditions for the repurchase are favorable.
(c) there are no material differences in the financial condition of the Company referenced in the last publicly reported balance sheet date that have not been publicly disclosed.
(d) there are no material differences in the consolidated results of core operations of the Company for the current quarter and the average for the four most recent quarterly periods that have not been publicly disclosed.
(e) it is anticipated that expected earnings for the current quarter will not be materially different from analysts' publicly announced estimates for the current quarter or guidance provided by the Company, if any.
(f) the Company is not currently in the process of conducting a transaction or series of related transactions that have not been publicly disclosed and which, if consummated, would likely have a material impact on the financial condition or results of operations of the Company, nor is the Company actively considering any such transaction or series of transactions.
(g) the stock repurchases are conducted in accordance with the currently effective stock repurchase program and are not being conducted for the purpose of manipulating the trading market for Company common stock; and
(h) the President and Chief Executive Officer or his designee(e) has sought the advice of any advisors as he shall deem appropriate.

Confidentiality

Serious problems could develop for the Company through unauthorized disclosure of inside information about the Company, whether or not for the purpose of facilitating improper trading of the Company's stock.

A. Confidentiality of Non-public Information.

Directors, officers, and employees of the Company should not discuss internal matters or developments with anyone outside of the Company (including family members, securities analysts, individual investors, members of the investment community and news media), except as required in the performance of regular corporate duties. In addition, directors, officers, and employees of the Company with knowledge of material, non-public information should only disclose such information to other Company personnel on a" need-to-know" basis so that the group of individuals with knowledge of material, non-public information is kept as small as possible.

All inquiries about the Company made by the financial press, investment analysts or others in the financial community, or by shareholders must be handled in accordance with the Company's Policy on Fair Disclosure to Investors. If you have any doubt as to your responsibilities under this policy, you should seek clarification from the Corporate Secretary before acting.

B. Prohibition Against Internet Disclosure

It is inappropriate for any unauthorized person to disclose Company information or to discuss the Company on the Internet, including in any forum or chat room where companies and their prospects are

discussed. The posts in these forums are, in some cases, made by investors who are poorly informed, who have malicious intent, or who intend to benefit their own stock positions. In order to avoid the disclosure of material and inside information, no director, officer or employee may discuss the Company or Company-related information in an Internet forum or chat room, regardless of the situation.

Insider Trading Policy Approved by the Board of Directors 12/07/2021

ATTACHMENT E -

WHISTLEBLOWER PROCEDURES AND POLICY

Statement of Principles

The Board of Directors of CCB and Coastal Financial Corporation (the "Company") has constituted and established an Audit Committee (the "Committee") with the authority, responsibility and specific duties as described in the Company's Audit Committee Charter. Pursuant to the Audit Committee Charter, the requirements of the Sarbanes-Oxley Act of 2002 and the rules and regulations of the Securities and Exchange Commission, the Committee is required to establish the procedures for (1) the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters ("Accounting Matters"), (2) the receipt, retention and treatment of complaints regarding potential violations of applicable laws, rules and regulations or of the Company's codes, policies and procedures ("Compliance Matters") and (3) the confidential, anonymous submission by employees of concerns regarding questionable Accounting Matters and Compliance Matters. In order to facilitate the reporting of employee complaints, the Committee has adopted this Whistleblower Procedures and Policy (this "Policy").

Pursuant to this Policy, any employee of the Company may submit a good faith complaint regarding Accounting, Compliance or Employee matters to the Company's management without fear of dismissal or retaliation of any kind. The Company is committed to achieving compliance with all applicable laws, rules, regulations, standards, and policies, including securities laws and regulations, accounting standards, accounting controls, audits, and Human Resource practices. The Committee will oversee treatment of employee concerns in this area.

Scope of Matters Covered by These Procedures

These procedures cover employee complaints relating to any questionable Accounting standards and controls, Audit and Human Resource practices, including, without limitation, the following:
Fraud or deliberate error in the preparation, evaluation, review, or audit of any of the Company's financial statements.
Fraud or deliberate error in the recording and maintenance of the Company's financial records.
Deficiencies in or noncompliance with the Company's internal accounting controls.
Misrepresentation or a false statement to or by a senior officer regarding a matter contained in the Company's financial records, financial statements, audit reports or Human Resource records; and
Deviation from full and fair reporting of the Company's financial condition.
In addition, these procedures cover employee complaints relating to any questionable Compliance Matter, including, without limitation, the following:

Applicable laws, rules, and regulations.

Listing standards of the NYSE MKT LLC applicable to domestic listed companies; and

The governance documents and policies of the Company, such as the Company's Code of Ethics and Corporate Governance Guidelines.

Reporting Procedures for Employee Complaints
Employees with concerns regarding questionable matters should share their questions, concerns, suggestions, or complaints with someone who can address them properly. In most cases, an employee's direct manager is in the best position to address an area of concern. However, if an employee is not

comfortable speaking with his or her manager, or if he or she is not satisfied with the manager's response, the employee is encouraged to speak with Human Resources and/or anyone in management with whom they are comfortable approaching. Managers are required to report questionable complaints to Human Resources and/or the Chairman of the Audit Committee.

When an employee is not satisfied or comfortable with the above stated escalation policy, employees should report complaints to the Audit Committee and Human Resources directly through an anonymous whistleblower hotline. The hotline number is **833-222-3893**, and can be reached 24 hours a day, seven days a week. Additionally, employees can access the hotline online at **www.lighthouse-services.com/coastalbank**

Treatment of Complaints
Upon receipt of a complaint, Human Resources and the Chairman of the Audit Committee will (1) determine whether the complaint actually pertains to Accounting, Compliance or Human Resource matters and (2) when possible, acknowledge receipt of the complaint to the sender.

Complaints relating to Accounting and/or Compliance matters will be reviewed by Human Resources and the Company's non-executive Chairman of the Board, the Chairman of the Audit Committee, the Internal Auditor, or such other persons as the Committee determines to be appropriate. Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review.

The Company will not discharge, demote, suspend, threaten, harass or in any manner discriminate against any employee in the terms and conditions of employment based upon any lawful actions of the employee with respect to good faith reporting of complaints regarding Accounting, Compliance or Human Resource matters or otherwise as specified in Section 806 of the Sarbanes-Oxley Act of 2002.

Reporting and Retention of Complaints and Investigations
Human Resources and/or the Company's non-executive Chairman of the Board and/or the Chairman of the Audit Committee will maintain a log of all complaints, tracking their receipt, investigation and resolution and shall prepare a periodic summary report for the Committee. Copies of the complaints and the log will be maintained in accordance with the Company's document retention policy.

Amendments

The Committee may amend these procedures at any time, consistent with the requirements of applicable laws, rules, and regulations.

Policy Statement on Whistleblower Claims The Board of Governors of the Federal Reserve System (Board) is issuing this policy statement to promote the submission of whistleblower claims regarding misconduct, unsafe or unsound practices, or violations of law or regulation occurring at any banking organization supervised by the Federal Reserve. The Federal Deposit Insurance Act protects employees of depository institutions from retaliation for providing whistleblower information to any federal banking agency or to the United States Department of Justice and provides rewards for whistleblowers in appropriate circumstances. 1 All persons are encouraged to report to Federal Reserve staff any information regarding any banking organization the Federal Reserve supervises or any director, officer, or employee of such banking organization that may have engaged in unsafe or unsound practices, violations of law or regulation, or violations of any orders or written agreements issued by the Federal Reserve ("whistleblower claims"). Whistleblower claims may be submitted by telephone, e-mail, or by form submission on the "contact us" page on the Board's webpage, or to any Federal Reserve supervisory staff. 2 The Board's Ombuds Office, 3 which is independent of the Federal Reserve's

supervisory functions, will ensure the intake of whistleblower claims is conducted confidentially and assist in processing these claims. Whistleblowers may elect to report anonymously. If known, the Federal Reserve will protect the whistleblower's identity as confidential. The identity and information will generally not be disclosed, including in response to Freedom of Information Act requests. There are, however, certain circumstances where the identity or information could be disclosed, including as a referral to or in response to requests from other federal or state financial institution supervisory agencies, or law enforcement agencies, in response to federal or state grand jury, criminal trial, or government administrative subpoenas, a court order, or other legal process. 4 By law, insured depository institutions may not discharge or otherwise discriminate against whistleblowers for providing information to the Federal Reserve. 5 In addition, the Federal Reserve does not tolerate retaliation against any whistleblower. The Federal Reserve takes seriously claims of retaliation against whistleblowers, and any claim of retaliation should be reported to Federal Reserve staff. If a whistleblower satisfies all the statutory requirements, and the Attorney General concurs, the Board, in its sound discretion and in appropriate circumstances, may reward the whistleblower with a sum of no more than the lesser of (i) 25 percent of the amount of the fine, penalty, restitution, or forfeiture collected; or (ii) $100,000. 6 While such rewards are possible, there is no assurance that a reward will be paid and no determination about a reward can be made until the conclusion of any action following an investigation. 7 Consumers seeking assistance with or seeking to submit complaints regarding their consumer accounts, products, or services provided by banking organizations supervised by the Federal Reserve should contact the Federal Reserve Consumer Help Center. 8 Persons wishing to report information relating to suspected fraud, waste, abuse, or mismanagement in the operations of the Federal Reserve System should contact the Office of Inspector General. 9 Reserve Banks are asked to distribute this letter to the supervised banking organizations in their districts and to appropriate supervisory staff. In addition, questions from potential whistleblowers may be submitted to the Board's Ombuds Office, https://www.federalreserve.gov/aboutthefed/ombuds.htm

Approved by the Board of Directors 12/14/2022

ATTACHMENT F –

REMOTE EMPLOYEE AGREEMENT

Remote work is a flexible work schedule arrangement, which permits employees to work at home or at a satellite office, or both. Employees are connected to the office by telephone and computer.

Being a remote employee is not for everyone. Employees may find they miss the stimulation of working in an office environment with a lot of human interaction. It is not a substitute for childcare or elder care. If you have small children or are providing primary care for an elderly adult, you will need to arrange for childcare or elder care during your agreed upon work hours. This agreement sets forth the conditions under which your remote employee program is sponsored by CCB. This agreement does not change the basic terms and conditions of your employment. You will remain subject to the same employment policies and procedures set forth in the CCB handbook. This agreement may be modified by CCB at its sole discretion and there may be times when you are required to spend more time than planned in the office upon CCB's request.
Your salary, job responsibilities and benefits do not change because of participation in a remote employee arrangement.

Performance location: The employee's remote work location will be the home address the employee has indicated in their employee record. If the remote employee intends to move to a new home address, they must notify Human Resources prior to moving. If the remote employee is traveling or working at an alternate remote location, they must request this in advance to their manager and Human Resources for approval. Travel destinations and alternate locations must be communicated with their manager for security purposes and system compatibility. Failure to comply with this provision may result in termination of the remote employee agreement and/or other appropriate disciplinary action.

Duration: This agreement will be valid beginning from the employee's start date and may be discontinued by either party with 30 daysnotice. The parties expressly acknowledge that nothing herein changes or modifies the employee's at-will employment status.

Internet Access: Employee must have access to reliable internet that is dedicated and secured at their primary work location address throughout their entire work shift. Minimum internet connection requirements for access are 10 mbps - download and 1 mbps - upload. A speed test is required. Satellite internet access cannot be supported.

Work assignments/Schedules: The employee will meet with their manager to receive assignments and to review completed work as necessary or appropriate. The employee will complete all assigned work according to work procedures mutually agreed upon by the employee and their Manager. Employees must attend all office meetings as requested as well as check voicemail, text, and e-mail regularly. The employee will work the schedule assigned to them by their manager. The assigned work schedule is subject to change, depending on business needs.

Logging Work hours: Non-exempt employees must log all daily working hours into the payroll system and take all required breaks. Notify your manager when leaving your remote employee location as you would inform others when leaving the office during the workday.

Trainings: Employees are required to complete web-based and virtual trainings as assigned. Trainings will include required compliance courses and core system courses through companywide Learning Management Systems. Additional trainings will be communicated through internal sources such as the bank Intranet or external resources.

Leave: All leave and travel will be based on the employee's primary business location. Employees must obtain approval before taking leave in accordance with established Coastal policies. By signing this form, employee agrees to follow established procedures for requesting and obtaining approval of leave.

Overtime: A non-exempt employee who works overtime is compensated in accordance with applicable law and rules. The employee understands that all overtime work must be approved in advance. By signing this agreement, the employee agrees that failing to obtain proper approval for overtime work may result in removal from the remote employee program or other appropriate action.

Equipment: Any equipment, software, or data provided by CCB for use in your home remains the sole property of CCB and may only be used for business purposes. Employees are expected to use the CCB supplied equipment to perform work, access systems, join meetings, etc. CCB computers may not be used for personal matters, and CCB owned software may not be duplicated. No household member or anyone else is permitted to use CCB equipment or software. All equipment must be returned to CCB in the original boxes upon request, in the event of an extended leave, upon resignation or termination, or if the telecommute program ends. In any event, you can either return the equipment yourself or arrange for a CCB representative to pick it up from your home. If the remote employee fails to ship their equipment within 7 days of termination, the equipment costs may be deducted from their final paycheck.
All equipment provided should be placed where it has adequate support and is connected to properly grounded electrical outlets. Keep all wires away from walkways. CCB accepts no responsibility for loss, damage, or repairs of employee-owned equipment.
Inspection: Employee must maintain a designated remote employee space free of recognized safety hazards. The remote employee location may be inspected periodically to ensure that proper maintenance of CCB equipment is performed, and that safety standards are met. Notice must be given to the employee at least 24 hours in advance of the inspection, which must occur during normal working hours.

Liability: CCB will not be liable for damages to the employee’s property or to third parties that result from participation in the remote employee program. In the event CCB is found liable in tort for injury to any person resulting from participation in the remote employee program, the employee agrees to indemnify and hold CCB harmless for any such loss resulting in injury to any person.

Reimbursement: CCB will not be responsible for operating costs, home maintenance, or any other incidental cost
(e.g., utilities) whatsoever, associated with the use of the employee's residence. The employee does not
relinquish any entitlement to reimbursement for authorized expenses incurred while conducting business for CCB.

Accommodations: As needed on an individual basis, CCB will review reasonable

accommodations requested by remote employees and human resources will determine if the remote employee can or cannot be accommodated.

Workers' Compensation: The employee is covered under the Workers' Compensation law if injured while performing official duties at the remote employee location.
Compliance with Federal, State and Local Laws: Employee certifies that the remote employee location complies with federal, state, and local laws relating to environmental and workplace safety, as well as state and local zoning, land use and building codes.
Coaching and Communication: The employee will meet with their manager in person or virtually on a regular consistent basis to establish honest and open feedback and communication to discuss what is working well and what challenges are being presented. These coaching sessions will be documented. Employee will need to meet established job standards and goals (as attached) and provide progress reports of work completed by coaching with manager weekly.
Records: The employee will apply approved safeguards to protect CCB records from unauthorized disclosure or damage. Work done at the remote employee location is considered CCB business. All records, papers, computer files, and correspondence must be safeguarded for their return to the primary business location. The employee agrees to comply with all applicable CCB privacy and confidentiality policies.

Moving: If the remote employee is planning on moving, they must notify Human Resources 30 days prior to moving. The new location must be assessed for compatibility. A new speed test will be required at the new location and must meet connection requirements as well.
Inclement Weather: If remote employees experiences any of the following issues listed below due to inclement weather, remote employees should notify their manager if they are unable to work:

- The threat of poor conditions, such as serious weather warnings
- Power outage or loss of other essential services
- An employee who has suffered damage to their home during inclement weather

Security: CCB and customer information must be protected from unauthorized or accidental access, use, modification, destruction, or disclosure using locked file cabinets and desks, regular password maintenance and other appropriate steps. Restricted-access materials may not be taken out of the CCB office or accessed through the computer unless approved in advance by your manager. No CCB work can be done on your own personal home computer, except through the use of Citrix. All hard copies of confidential information should be discarded by using a shredder.

Costs: CCB agrees to pay for postage and shipping of CCB equipment, and office supplies such as notebooks, pens, pencils, and sticky notes. Reasonable requests for office supplies may be made to Human Resources. These costs must be requested and approved through Human Resources. CCB also provides a technology stipend per month for remote employees.
CCB is not responsible for costs associated with the initial set-up of a home office, such as remodeling, repairs, lighting, or new furniture, nor for any home-related expenses such as heating/air conditioning or electricity.
This Remote Employee Agreement may be discontinued at any time by either you or CCB with a 30-day notice of such a change. There may be instances, however, where no notice is possible. If your job performance suffers under the remote employee arrangement, you will be required to return to the office. If you choose not to return, your response will be considered a voluntary resignation.

ATTACHMENT G -

ACCEPTABLE USE POLICY

Introduction

Coastal Community Bank has established a set of policies to help protect bank resources, as well as nonpublic bank and customer information. Many of these policies address appropriate behavior, use of technology resources, and operational procedures as they pertain to employees. Although not all conceivable situations can be specifically addressed, this Acceptable Use Policy addresses those policies and provides guidelines for you, the user.

If you ever have any question regarding acceptable use or behavior, it is your responsibility to consult your supervisor or a member of bank management. Failure to comply with these policies may lead to disciplinary action, up to and including termination.

Technology Resources

Technology resources include, but are not limited to, the following:

Computer systems

Removable media such as:

- CDs
- DVDs
- MP3 Players
- Jump Drives

Computer software

Internet access

Email

Telephones

Voicemail

Mobile phones

Nonpublic Information

Nonpublic information includes, but is not limited to, the following:

Social Security number

Account number

Personal identification number

Account password

Policies

Acceptable Use of Information Assets

Inappropriate Use

Do not use technology resources for unauthorized purposes such as:

For personal or financial gain

In violation of bank policy

In violation of copyright laws

For actions contrary to the best interest of the bank, including disclosure of confidential or proprietary information of the bank or third parties

To display, access, download, distribute or reproduce sexually explicit or pornographic material

To access streaming media (videos, music, webcasts, etc.)

Appropriate Use

Appropriate use of technology resources includes using resources for official business or with prior authorization from senior management.

Personal Use

Occasionally, employees may need to use technology resources for personal use. Senior management approval must be obtained prior to use and, unless noted otherwise, approval must be obtained ***each*** time.

Personal use of the bank's technology resources (Internet, computers, printers, etc.) without appropriate authorization will be grounds for disciplinary action and possible termination.

Coastal Community Bank assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over, or stored on, any bank resource. In addition, Coastal Community Bank accepts no responsibility or liability for the loss or non-delivery of any personal email or voicemail.

Telephone System Use

Occasional, brief personal calls may be made or taken at your desk. Do not make personal long-distance calls using the bank telephone system, except in the case of an emergency. If you must make such a call, either use a personal cell phone or notify your supervisor prior to making the call. Provide adequate call details to your supervisor including:

Date

Time

Number called

Duration of the call

Management reserves the right to request reimbursement for personal long-distance calls.

Access and Monitoring

Any data stored on any bank resources are considered the property of Coastal Community Bank. This includes, but is not limited to, the following:

Email

Programs

Data files (e.g., Word documents, spreadsheets, etc.)

Voicemail

As such, you can have no expectation of privacy concerning personal data that may be stored on any bank resource. Coastal Community Bank reserves the right to access and monitor any of its technology resources, files, and communications at any time and for any reason, as deemed necessary by senior management, which may include:

Verification of compliance with policies

For purposes of legal proceedings

To investigate misconduct

To locate information

At no time are you to monitor technical resources without prior authorization from senior management.

At no time are you to access customer/bank information that is not directly related to performing your duties within the bank.

No photographs are to be taken inside bank facilities without prior authorization.

Internet Access

Only use Internet access for business purposes unless otherwise authorized by senior management.

Coastal Community Bank reserves the right to limit access to the Internet to those who need it to perform their job duties. Coastal Community Bank also reserves the right to monitor, log, and review Internet usage. This includes, but is not limited to, the following:

Blocking certain sites considered offensive

Monitoring Internet usage rates

Monitoring sites accessed and the duration of time spent at certain sites

Trying to circumvent Internet access settings will be grounds for termination.

Cloud Computing

Do not use cloud services for business purposes without approval from the IT Steering. Use of unapproved cloud services can result in security deficiencies and unauthorized access to sensitive data.

Examples of cloud services which require approval for business use include:

File exchange, storage, and sharing applications

Messaging applications

Productivity applications

Video conferencing applications

If use is approved, encrypt sensitive information prior to transmitting via the internet.

Data Retention and Destruction

Do not discard anything containing sensitive information into a trash can. Either shred the data or place it in a shred bin. This includes, but is not limited to, the following:

Account statements

CDs containing customer / bank information

Any document containing nonpublic information

Data Storage

All data should be stored on a network drive designated by senior management. If you do not know what drive to save data on, consult your supervisor. Do not store data on your workstation unless authorized to do so by senior management. Data includes:

Spreadsheets

Word documents

Scanned images

Data stored on workstations is not backed up and cannot be recovered if the workstation is unavailable. In addition, access is not restricted on data stored on a workstation and, therefore, could result in confidential information being accessed by unauthorized individuals.

If you have data stored on a workstation, move it to the designated network drive. If you discover data stored on a workstation which is not your own, notify your supervisor.

Do not store data not directly related to your job function or business activity of the bank (e.g., animations, audio files, etc.).

Email Security

Access to email, using bank systems and facilities, is intended for business use only unless approved by senior management. Any email created or stored on bank resources is considered property of Coastal Community Bank. At the discretion of senior management, it may be accessed and viewed for any reason and at any time.

Do not access personal email on bank systems. This includes, but is not limited to, the following:

Yahoo Mail

Hotmail

Gmail

Email accounts hosted by your residential Internet Service Provider (ISP) by using:

Outlook

Microsoft Mail

The following email guidelines apply to all users:

Do not attempt to read, modify, or delete email not addressed to you unless it has been determined appropriate by senior management.

Do not participate in any form of chain letter.

Do not send email appearing to come from someone else.

Do not send email with any proprietary, confidential, or otherwise sensitive information unless approval has been obtained from senior management, and the email is encrypted.

Do not send email containing statements or contents that are defamatory, offensive, harassing, illegal, derogatory, or discriminatory. This includes, but is not limited to, the following:

Messages based on race, gender, religion, or nation origin

Sexually explicit messages, images, cartoons, or jokes

Foul, inappropriate or offensive messages

If you receive an offensive email, request the sender stop sending such material. If the email messages continue, report the incident to your supervisor.

When communicating with customers via email, do not send confidential information. If a customer sends an email containing sensitive customer information, erase that information prior to responding. If a customer sends an email requesting sensitive customer information, respond to the customer using wording similar to the following:

Thank you for using Coastal Community Bank. We have received your recent email and look forward to providing you the best service possible. Due to security concerns involving identity theft, bank policy prohibits sending any of your personal information in an unsecured email message. Therefore, I will attempt to contact you via phone or mail using the phone numbers and address in our system, or you may call us or come by one of our bank locations.

If you attempt to contact the customer, refer to customer identification procedures (CIP).

8.5.7

Encryption

Do not encrypt data or protect files with passwords unless authorized to do so by IT Management. This authorization should also include procedures or instructions on how and where to securely log the password or encryption key.

Authorization and procedures regarding password logs and encryption keys are necessary to ensure any bank or customer data can be accessed or recovered when needed. Without proper procedures, data stored in an encrypted form may not be recoverable later.

Malicious Software Protection

All files that are downloaded, either from the Internet or from email, must be scanned for malicious software. Coastal Community Bank has taken measures to thwart intrusions by unauthorized persons. It is extremely important that these systems be maintained.

Anyone who attempts to bypass these security measures, or who knowingly tries to propagate infected files will be subject to legal action, in addition to disciplinary action, up to and including termination.

If you suspect that a bank system may have malicious software, notify your supervisor immediately.

Messaging

Do not communicate via instant messaging applications between users on the Internet.

Do not participate in forums or message boards unless it is for business purposes and has been authorized by senior management.

Mobile Devices

Do not use your mobile phone to make personal phone calls or to send text messages, except during breaks or away from customers, without prior approval from your supervisor.

All mobile phones must be turned off or set to vibrate mode during business hours.

Do not connect a mobile device to the bank network or receive/transmit bank or customer data without approval by senior management. Mobile devices include, but are not limited to, the following:

Cellphones

Smartphones

Tablets

Laptops

Bluetooth devices

If you have received authorization to use a mobile device, whether bank-owned or personally-owned, to store or process bank or customer information, you are expected to take every possible precaution to prevent unauthorized access or theft of the device. Mobile devices present a unique security risk, since they are normally carried outside the facility, and may contain sensitive information; therefore, the following guidelines apply:

Do not modify the device hardware or software in a way that would circumvent security controls (e.g. jailbreaking, rooting, etc.).

Only data approved by senior management can be stored on the mobile device.

If sensitive data is stored on the device, commercial grade encryption software must be used.

When turned on, the mobile device must require authentication before access to any bank or customer information is allowed.

Ensure any approved Bluetooth-capable devices are not in discovery mode, except when pairing with another device.

Download mobile applications only from reputable stores authorized by the device manufacturer (e.g., Apple's App Store, Google Play, and the Windows Store).

If you have received authorization to use a personally owned mobile device for bank business (including sending/receiving email, remote processing, etc.), the bank reserves the right to:

Enable remote wipe and will wipe the device if any of the following apply:

The device is lost or stolen.

Employment is terminated.

The device is believed to have been compromised, breached, or infected with a virus.

Enable the device to lock after a period of inactivity.

Automatically erase the device after a specified number of invalid logon attempts

Physically inspect the device and remove any bank or customer data

Initialize the device in such a way that all bank and/or customer data is removed (e.g., reset to factory settings or format the hard drive and reinstall the operating system, etc.)

Retain any rights to the phone number for a mobile phone covered under the bank's service plan with a mobile carrier

If your mobile device is lost or stolen, notify the IT department immediately.

Driving Safely

Employees are prohibited from using Bank issued mobile devices while driving. Unless using Bluetooth, before using a Bank issued mobile device while driving, employees are expected to pull off to the side of the road and safely stop the vehicle. Employees are expected to abide by all applicable laws covering the use of Bank issued mobile devices while driving regardless of whether the vehicle is a Bank-Owned vehicle.

CL to IL (Corporate Liable to Individual Liable)

It is the Bank's policy that the wireless numbers associated with all Bank issued Smartphone and Cell Phone devices are Bank owned. There will be no approval granted to an employee to seize their wireless number upon separation from the Bank. Employees may elect to transfer their personal number to the Bank issued mobile device. If an employee that transferred their personal number to the Bank separates from the Bank and wishes to transfer their number back to a personal device, approval will not be granted.

Employee Termination

If employment is terminated all bank owned mobile devices and their components must be returned to Coastal Community Bank.

Policy Authority and Enforcement

The Bank's SVP of IT is responsible for the development and oversight of these policies and standards. The SVP of IT works with Senior Management, Human Resources, the Information Security Officer, Audit Services, Compliance, Legal, and others for development, monitoring and enforcement of these policies and standards.

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the Bank and/or action in accordance with local ordinances, state or federal laws.

Physical Security of Sensitive Information

Utmost discretion in the handling of all bank data and confidential or proprietary information of customers and third parties is very important. Never provide proprietary, confidential, or otherwise sensitive information to unauthorized individuals. To the extent practical, the following guidelines apply:

Close files and keep paperwork face down on the desk to help prevent the inappropriate display of confidential information.

At the end of the workday, leave desks in a clean, organized manner, with confidential information secured in a desk or other appropriate location.

Avoid removing confidential data (on paper or electronic media) from a workspace unless required for work purposes, and only with appropriate safeguards for the data.

Avoid discussing confidential data outside the purview of specific job functions.

Avoid speaking in a loud tone when discussing confidential data in a public area.

Write balances on paper rather than saying amounts verbally.

Be wary of social engineering attempts to gain access to confidential information or to acquire the means of accessing confidential information.

Position visible computer screens away from unauthorized individuals; utilize computer privacy screens as necessary.

Clear computer screens when finished viewing confidential data.

Lock the computer workstation (such that a password is required to regain access) before leaving the workstation.

Log off computer workstations when they are no longer needed.

Verify the identity and authorization of anyone requesting access to secured areas of the bank.

Remote Access

Do not connect a modem to workstations on the bank network. Senior management must approve all modems prior to connection.

At times, it may be necessary to connect to the bank network from outside the bank facilities. If you need to connect to the network remotely, ensure the computer you will be using, whether it is the bank's computer or a non-bank device (e.g., computers, mobile phones, etc.), has all patches installed, as well as a current copy of approved anti-malware software. Obtain authorization from senior management prior to accessing the network remotely.

Remote Work

Confirm with your supervisor whether you are authorized to work remotely. If you receive authorization, follow these recommendations to secure your remote work devices and environment.

Only use authorized devices for remote work.

To secure remote work devices:

Install operating system, software, and firmware patches in a timely manner.

Do not disable security features (e.g., lock screens, encryption, anti-malware, etc.).

Do not install or use unauthorized applications (e.g., video conferencing, messaging, file sharing, etc.).

Do not use unauthorized removable media (e.g., flash drives, memory cards, compact disks (CDs and DVDs), external hard drives, smart devices, etc.).

Do not store sensitive bank or customer data on the devices. Store such data on a network drive controlled by the bank and designated by senior management.

Secure devices when they are not in use.

- Screen lock or shut down devices, such that authentication is required to regain access.
- Do not leave devices unattended in a public or shared area.
- Do not allow other individuals (e.g., family members, roommates, friends, etc.) to use devices.

To ensure the physical security of sensitive bank or customer information at remote locations:

Do not print documents containing sensitive bank or customer information.

Personal printing devices may be used with approval from senior management.

Store physical documents in a secure manner (e.g., locked in a safe, drawer, cabinet, etc.), when not in use.

Destroy physical documents in accordance with bank policy, when no longer needed.

If a security incident is suspected or known to have occurred, you should:

Disconnect potentially affected devices from the bank network and internet.

Keep devices powered-on to preserve evidence.

Report the incident to your supervisor immediately.

Removable Media and Data Transfer

Do not remove data from the bank network without authorization from the IT Staff. This includes, but is not limited to, the following:

Transferring files to any form of removable media (e.g., CDs, tapes, jump drives, etc.)

Emailing files as attachments

Removing data from the network increases the chances of confidential information being exposed to unauthorized individuals. Therefore, any confidential data that has been authorized must be encrypted on any removable media.

Do not copy data to the bank network without authorization from the IT Staff. This includes, but is not limited to, the following:

Saving email attachments

Transferring data from any form of removable media (e.g., CD, tape, jump drive, etc.)

Copying data to the network can introduce malicious software and endanger the entire network and workstations.

Reporting of Security Violations

If you suspect or are aware of a violation of any of these policies, report it to your supervisor immediately. If you feel reporting this to your supervisor is inappropriate, you should report it to the Information Security Officer.

Social Media

Employees are not allowed to access personal social networking accounts from any bank system without prior approval from senior management.

Employees are not allowed to associate their bank email address with any social networking site without prior approval.

Employees are not allowed to make statements on behalf of the bank without prior approval.

Any information posted on social networking sites regarding bank products, promotions, services, etc., is considered advertising and must be approved prior to posting.

Blogging and posting to social media sites by employees, whether using Coastal Community Bank's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.

Employees are prohibited from revealing any Coastal Community Bank confidential or proprietary information, secrets, customer information, or any other material covered by the Information Security Policy when engaged in blogging or posting to social media sites.

Employees shall not engage in any blogging or posting to social media sites that may harm or tarnish the image, reputation, and/or goodwill of Coastal Community Bank and/or any of its employees or customers.

Employees are prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or posting while representing Coastal Community Bank or from Coastal Community Bank assets.

Employees may also not attribute personal statements, opinions, or beliefs to Coastal Community Bank when engaged in blogging or posting. If an employee is expressing his or her beliefs and/or opinions in blogs or social media sites, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Coastal Community Bank. Employees assume any and all risks associated with blogging and posting.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Coastal Community Bank's trademarks, logos, and any other Coastal Community Bank intellectual property may also not be used in connection with any unauthorized blogging or posting activity.

Software Licensing and Installation

Do not install any personal software on any bank system.

If software has been purchased for you, DO NOT install it yourself unless you have received authorization to do so by the IT Department.

Do not download software from the Internet without approval from the IT Department. If software is downloaded from the Internet, ensure proper licensing is obtained and forwarded to the IT Staff. This includes, but is not limited to, the following:

Games

Audio files

File and music exchange programs (peer-to-peer applications)

Software applications

User Authentication

Each user will have their own username and password to access the network and other applications. Unless instructed otherwise by your supervisor, always use your own username. You are personally responsible for all activities performed with your user accounts. Therefore, it is imperative that you NEVER give your password to anyone. If you must document your password, store it in a secure location, inaccessible by others.

Do not attempt to obtain access to another user's account by trying to use their name/password without prior authorization from management. This includes:

Attempting to guess the username/password

Using logon name/password you already know

Using any other unauthorized means to determine the username/password

Management may evaluate passwords at any time to ensure your password follows the following guidelines:

Do not use any names (e.g., your first name, your middle name, your last name, your logon name, spouse's name, children's name, etc.). This includes:

Using the name as is (e.g., username)

Spelling the name backwards (e.g., emanresu)

Using all capital letters (e.g., USERNAME)

Doubling the name (e.g., usernameusername)

Do not use common information (e.g., license plate number, address, driver's license number, social security number, telephone number, brand of automobile, etc.).

Do not use common words (words found in a dictionary).

Do not use repeating characters or single digits:

11111111

aaaaaaaa

Make your password easy to remember.

Consider using a "pass phrase" as a password.

Thi5isalong&strongpassword!!

Pass phrases are memorable.

Use a minimum of 12 characters for your passwords.

Use both upper and lower case letters (e.g., A,a,B,b, etc.).

Use non-alphanumeric characters (e.g., 1, 2, 3, !, @, etc.).

Do not use the same password for personal sites (including social networking sites) as you do for bank passwords.

Wireless Network Access

Do not connect wireless access devices, such as wireless access points or routers, to the bank's network without approval by IT Management.

EMPLOYEE HANDBOOK ACCEPTANCE STATEMENT
INCLUDING ALL ATTACHMENTS

The contents of this handbook are a summary of current employment standards, policies, and guidelines at CCB. CCB reserves the right to modify, amend or terminate any provision contained in this manual at any time without advance notice. Any such changes or addendums made by CCB will immediately supersede the current contents of this manual.

This manual describes general guidelines, and nothing contained in this manual is intended to create an employment contract either expressed or implied between CCB and any of its employees for any definite term of employment or for the provision of any benefits or procedures described in this handbook

Employees at CCB are hired for indefinite terms of employment. CCB is an at-will employer, which means that the employee or CCB may terminate the employment relationship at any time, with or without reason and with or without notice.

No agent or representative of CCB other than the President and/or a member of the Senior CCB Leadership Team, and then only in writing, has any authority to enter into any agreement for employment for any specified period of time, or to enter into any employment agreement that in any way modifies the at-will status of employment at CCB.

My signature whether electronic or manual, indicates that I understand my obligation to read and understood the foregoing paragraphs and that I have received a copy of the CCB Employee Handbook.

Employee Signature

_____

Date

_____

Employee Printed Name

_____