National Bank for Agriculture and Rural Development

NABARD

CYBERSECURITY HANDBOOK 2.0

Strategies for Effective
Cyber Defense

TABLE OF CONTENTS

Database Security

Database security uses policies and controls to protect data against unauthorized access, attacks, and loss, ensuring confidentiality and integrity.

Incidents Management

Incident management is the systematic process of detecting, analyzing, and resolving security threats to minimize business impact and ensure recovery.

Third Party Security Management

Third-party security management identifies, mitigates, and monitors risks from vendors and partners to protect data, systems, and compliance.

Network Security

Network security uses technologies, controls, and policies to protect network integrity and data from unauthorized access, misuse, and cyberattacks.

Training and Awareness

Cybersecurity training and awareness educate individuals to recognize, prevent, and respond to cyber threats, reducing risks and enhancing organizational security.

Access Control and Patch Management

Access control restricts network access to authorized users/ devices, while patch management updates systems to fix vulnerabilities and enhance security.

Asset Management

Asset management is the continuous process of identifying, tracking, and securing an organization's digital and physical assets to mitigate risks and vulnerabilities.

NABARD

DATABASE SECURITY

THINGS TO DO

REGULARLY UPDATE

AS SOON AS PATCHES AND UPGRADES ARE AVAILABLE, USE THEM TO REMEDY SECURITY HOLES IN THE DATABASE ENGINE AND ANY SOFTWARE THAT WORKS WITH IT.

ENCRYPT DATA

TO KEEP PRIVATE INFORMATION SAFE FROM PERSONS WHO SHOULDN'T HAVE ACCESS TO IT, USE ENCRYPTION ON DATA THAT IS AT REST AND IN TRANSIT.

IMPLEMENT ACCESS CONTROL

USE ROLE-BASED ACCESS AND THE LEAST PRIVILEGE NOTION TO LIMIT WHO CAN SEE, CHANGE, OR DELETE DATA.

MONITOR ACTIVITY

TURN ON LOGGING AND CHECK AUDIT TRAILS OFTEN TO SEE IF SOMEONE IS MAKING STRANGE REQUESTS OR TRYING TO GET TO DATA WITHOUT PERMISSION.

DATABASE BACKUP

MAKE COPIES OF YOUR BACKUPS OFTEN AND STORE THEM SECURELY TO KEEP THEM SAFE. ALSO, CHECK TO SEE IF THEY ARE ENCRYPTED AND MAY BE RESTORED.

USE STRONG AUTHENTICATION

MAKE SURE THAT DATABASE ADMINS AND OTHER USERS WITH SPECIAL ACCESS USE MULTI FACTOR AUTHENTICATION.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

DON'T USE DEFAULT CREDENTIALS

RIGHT AWAY, CHANGE THE DEFAULT USERS AND PASSWORDS. FOR SECURITY, NOT DOING THIS IS QUITE RISKY.

DON'T KEEP SENSITIVE DATA IN PLAIN TEXT

DON'T KEEP YOUR PASSWORDS, PERSONAL INFORMATION, OR FINANCIAL INFORMATION IN PLAIN TEXT. INSTEAD, PROTECT THEM WITH ENCRYPTION.

DON'T GIVE USERS TOO MANY RIGHTS

ONLY GIVE USERS THE ACCESS THEY NEED AND ONLY GRANT THEM ADMIN RIGHTS IF THEY REALLY NEED THEM.

DATABASE SECURITY

DON'T DO IT!

DON'T IGNORE LOGS AND ALERTS

IF YOU DON'T CHECK LOGS, YOU COULD MISS BREACHES. YOU SHOULD ALWAYS LOOK INTO THINGS THAT SEEM STRANGE.

DON'T FORGET ABOUT BACKUP SECURITY

ATTACKERS LOVE BACKUPS THAT AREN'T PROTECTED. DO NOT KEEP THEM IN PLACES THAT ARE NOT SAFE OR EASY TO GET TO.

DON'T SKIP TESTING

ALWAYS MAKE SURE THAT YOUR DATABASE IS SAFE AND THAT YOU KNOW HOW TO RESTORE BACKUPS.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

INCIDENT MANAGEMENT

THINGS TO DO

SET CLEAR PROCEDURES

MAKE SURE THERE ARE CLEAR, WRITTEN STEPS FOR FINDING, REPORTING, AND FIXING PROBLEMS. EVERYONE SHOULD KNOW WHAT THEY NEED TO DO.

PRIORITIZE BASED ON IMPACT

TO MAKE SURE THAT THE MOST IMPORTANT THINGS ARE TAKEN CARE OF FIRST, SORT THEM BY HOW SERIOUS THEY ARE AND HOW THEY AFFECT THE FIRM.

MAKE A STRONG RESPONSE TEAM

GIVE SKILLED PERSONNEL DISTINCT ROLES, LIKE TECHNICAL RESPONDERS ETC., TO FORM A ROBUST REACTION TEAM.

USE AUTOMATION AND MONITORING TOOLS

USE TECHNOLOGIES THAT PROVIDE YOU ALERTS IN REAL TIME, CHECK LOGS, AND ISSUE TICKETS AUTOMATICALLY TO HELP YOU UNCOVER PROBLEMS AND FIX THEM FASTER.

KEEP YOUR RECORDS UP TO DATE

FOR FUTURE REFERENCE AND COMPLIANCE, MAKE SURE YOU HAVE CLEAR RECORDS OF WHAT HAPPENED, HOW YOU FIGURED OUT WHAT CAUSED IT, AND WHAT YOU DID TO RECTIFY IT.

DO POST-INCIDENT REVIEWS

AFTER AN INCIDENT, GO BACK TO SEE WHAT WENT WRONG, WHAT WORKED, AND HOW TO MAKE FUTURE REACTIONS BETTER.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

INCIDENT MANAGEMENT

DON'T DO IT!

DON'T WAIT TOO LONG TO RESPOND

TIME IS VERY IMPORTANT. THE LONGER YOU WAIT TO ACT, THE WORSE THE DAMAGE MAY GET AND THE LONGER IT WILL TAKE TO FIX.

DON'T SKIP DOCUMENTATION

IF YOU DON'T WRITE DOWN THE DETAILS OF AN EVENT, IT WILL BE HARDER TO FOLLOW THE RULES AND FIGURE OUT WHAT'S GOING ON LATER.

DON'T IGNORE SMALL ALERTS

SMALL PROBLEMS MEAN THAT BIGGER ONES ARE ON THE WAY. TAKE A LOOK AT THEM BEFORE THINGS GET OUT OF HAND.

DON'T FORGET TO TALK

WHEN PEOPLE DON'T TALK DURING AN EVENT, IT'S TOUGHER TO UNDERSTAND WHAT'S GOING ON. TELL FOLKS WHAT'S GOING ON IN A TIMELY MANNER SO THAT EVERYONE IS AWARE.

DON'T NEGLECT TRAINING

DON'T FORGET TO TRAIN YOUR TEAMS. IF THEY AREN'T TAUGHT, THEY CAN PANIC OR MAKE A MISTAKE DURING AN INCIDENT. TRAINING ON A REGULAR BASIS IS IMPORTANT.

DON'T FORGET TO CHANGE YOUR PLAN

AS SYSTEMS CHANGE, SO SHOULD YOUR PLAN FOR DEALING WITH DIFFICULTIES. MAKE SURE IT STAYS UP TO DATE.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

THIRD PARTY SECURITY MANAGEMENT

THINGS TO DO

DO A THOROUGH DUE DILIGENCE CHECK

BEFORE BRINGING ON A VENDOR, CHECK THEIR CERTIFICATIONS, PROCEDURES, AND HISTORY OF BREACHES TO SEE HOW SECURE THEY ARE.

SET CLEAR SECURITY REQUIREMENT

CONTRACTS AND SLAS SHOULD SPELL OUT WHAT IS EXPECTED IN TERMS OF CYBERSECURITY, SUCH AS ENCRYPTION STANDARDS ETC.

LIMIT DATA ACCESS

GIVE SUPPLIERS ONLY THE ACCESS THEY NEED TO EXECUTE THEIR JOBS, FOLLOWING THE CONCEPT OF LEAST PRIVILEGE.

SET UP INCIDENT RESPONSE PROTOCOLS

MAKE SURE YOUR PROVIDERS KNOW HOW TO REPORT AND HANDLE SECURITY PROBLEMS IN A WAY THAT WORKS WITH YOUR OWN IR PLAN.

KEEP AN UP-TO-DATE RECORD OF SUPPLIERS

MAKE SURE YOUR LIST OF ALL YOUR THIRD-PARTY PROVIDERS, THEIR ACCESS LEVELS, AND THE DANGERS THAT COME WITH THEM IS ALWAYS UP TO DATE.

TRAIN YOUR EMPLOYEES

SHOW THEM HOW TO DEAL WITH VENDORS THE RIGHT WAY AND HOW TO SPOT DANGERS FROM OUTSIDE SOURCES.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

THIRD PARTY SECURITY MANAGEMENT

DON'T DO IT!

DON'T ASSUME THAT SUPPLIERS ARE SAFE BY DEFAULT

EVEN WELL-KNOWN ONES CAN HAVE PROBLEMS. ALWAYS CHECK; DON'T JUST TRUST.

DON'T SHARE SENSITIVE DATA WITHOUT CONTROLS

DON'T LET ANYONE SEE SENSITIVE DATA UNTIL YOU SAY IT'S OKAY. KEEP AN EYE ON YOUR DATA AND USE ENCRYPTION TO KEEP TRACK OF WHO CAN GET TO IT.

DON'T SKIP CONTRACTUAL SAFEGUARDS

NOT INCLUDING SECURITY CLAUSES IN YOUR CONTRACTS COULD GET YOU IN LEGAL AND FINANCIAL TROUBLE.

DON'T FORGET ABOUT BREACH NOTIFICATION GAPS

MAKE SURE THAT PROVIDERS ARE REQUIRED TO TELL YOU RIGHT AWAY IF THERE IS A BREACH. A LOT OF PEOPLE DON'T DO THIS UNLESS THEY HAVE TO.

DON'T FORGET OFFBOARDING STEPS

WHEN A VENDOR CONTRACT EXPIRES, CUT OFF ACCESS RIGHT AWAY AND MAKE SURE THAT DATA IS SAFELY RETURNED OR DESTROYED.

DON'T IGNORE CHANGES IN VENDOR RISK

A VENDOR'S RISK PROFILE COULD CHANGE OVER TIME, SO DON'T THINK OF EVALUATIONS AS THINGS YOU PERFORM ONCE.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

NETWORK SECURITY

THINGS TO DO

IMPLEMENT STRONG ACCESS CONTROL

USE STRONG ACCESS CONTROLS TO LIMIT WHO CAN GET TO ESSENTIAL SYSTEMS. THERE ARE MANY WAYS TO DO THIS, INCLUDING ROLE-BASED ACCESS, MFA, AND THE PRINCIPLE OF LEAST PRIVILEGE.

DO REGULAR SECURITY AUDITS

CHECK YOUR NETWORK INFRASTRUCTURE EVERY SO OFTEN TO FIND WEAKNESSES AND MAKE SURE YOU ARE FOLLOWING THE RULES.

KEEP SYSTEMS UP TO DATE

USE PATCHES AND UPGRADES ON OPERATING SYSTEMS, FIRMWARE, AND APPLICATIONS TO FIX SECURITY HOLES THAT HAVE ALREADY BEEN FOUND.

ENCRYPT DATA IN TRANSIT AND AT REST

USE SECURE PROTOCOLS LIKE HTTPS, VPN, AND TLS TO KEEP SENSITIVE DATA FROM BEING STOLEN WHILE IT'S BEING TRANSFERRED OR STORED.

EDUCATE EMPLOYEES

SHOW YOUR EMPLOYEES HOW TO USE THE INTERNET SAFELY AND HOW TO RECOGNIZE PHISHING AND SOCIAL ENGINEERING. MOST OF THE TIME, THEY ARE THE WEAKEST LINK.

CHECK LOGS AND TRAFFIC

USE SIEM TECHNOLOGIES TO LOOK AT LOGS AND FIND PROBLEMS BEFORE THEY GET WORSE.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

NETWORK SECURITY

DON’T DO IT!

DON'T USE DEFAULT CREDENTIALS

CHANGE THE DEFAULT USERNAMES AND PASSWORDS RIGHT AWAY BECAUSE HACKERS TYPICALLY USE THEM.

DON'T LET ANYONE HAVE UNRESTRICTED ACCESS

ATTACKERS CAN EASILY GET INTO SYSTEMS THAT HAVE OPEN PORTS, UNSECURED WI-FI, OR BROAD PERMISSIONS.

DON'T FORGET ABOUT ENDPOINT SECURITY

ANYONE CAN GET IN THROUGH DEVICES THAT AREN'T PROTECTED. INSTALL ANTIVIRUS, EDR, AND PATCH MANAGEMENT.

DON'T FORGET ABOUT PHYSICAL SECURITY

MAKE SURE THAT ROUTERS, SWITCHES, AND SERVERS ARE PHYSICALLY SAFE FROM UNWANTED ACCESS.

DON’T ASSUME CLOUD SERVICES ARE AUTOMATICALLY SECURE

YOU SHOULD NEVER ASSUME THAT CLOUD SERVICES ARE SAFE BY DEFAULT. ALWAYS SET THEM UP CORRECTLY AND KEEP AN EYE ON THEM.

DON'T DELAY UPDATES

NOT INSTALLING PATCHES MAKES MACHINES VULNERABLE TO ATTACKS THAT ARE ALREADY KNOWN.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

TRAINING AND AWARENESS FOR CYBERSECURITY

THINGS TO DO

MAKE IT ONGOING, NOT ONE-TIME

SET UP REGULAR SESSIONS, LIKE ONCE A MONTH OR ONCE EVERY THREE MONTHS, TO REMAIN ON TOP OF EMERGING THREATS AND KEEP GOOD HABITS.

USE REAL-LIFE SITUATIONS

TO MAKE TRAINING MORE EFFECTIVE AND MEMORABLE, ADD PHISHING SIMULATIONS, FAKE BREACHES, AND HANDS-ON ACTIVITIES.

TEACH EMPLOYEES ABOUT POLICIES

MAKE SURE YOUR WORKERS KNOW THE RULES REGARDING HOW TO HANDLE DATA, PASSWORDS, WORKING FROM HOME, AND REPORTING DIFFICULTIES.

CREATE A CULTURE THAT PUTS SECURITY FIRST

TELL YOUR EMPLOYEES TO REPORT ANY STRANGE BEHAVIOUR WITHOUT BEING AFRAID. DON'T JUST FOLLOW THE RULES WHEN IT COMES TO CYBERSECURITY.

UPDATE CONTENT REGULARLY

MAKE SURE YOUR TRAINING MATERIALS ARE UP TO SPEED WITH EMERGING THREATS LIKE AI-GENERATED PHISHING, DEEPFAKES, OR CLOUD MISCONFIGURATIONS.

ENCOURAGE THE USE OF SECURITY TOOLS

TEACH YOUR WORKERS HOW TO SAFELY USE PASSWORD MANAGERS, VPNS, MFA, AND FILE-SHARING PLATFORMS THAT ARE SAFE.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

TRAINING AND AWARENESS FOR CYBERSECURITY

DON'T DO IT!

DON'T BLAME WORKERS FOR MAKING MISTAKES

DON'T MAKE PEOPLE FEEL BAD FOR CLICKING ON PHISHING LINKS OR MAKING MISTAKES. CONCENTRATE ON LEARNING AND GETTING BETTER.

DON'T THINK THAT ONE SIZE FITS ALL

GENERIC TRAINING DOESN'T ALWAYS WORK. CHANGE DEPENDENT ON HOW MUCH RISK YOU TAKE, WHAT YOUR PROFESSION IS, AND HOW GOOD YOU ARE WITH TECHNOLOGY.

DON'T USE JARGON

USE SIMPLE PHRASES AND PICTURES TO HELP NON-TECHNICAL STAFF COMPREHEND YOUR IDEAS BETTER.

DON'T FORGET ABOUT NEW HIRES

MAKE SURE THAT EVERY NEW EMPLOYEE GOES THROUGH SECURITY ONBOARDING, SO THEY START WITH THE CORRECT ATTITUDE.

DON'T TREAT IT LIKE A CHECKBOX EXERCISE

TRAINING SHOULD DO MORE THAN JUST MEET AUDIT CRITERIA; IT SHOULD ALSO RAISE TRUE AWARENESS.

DON'T FORGET TO FOLLOW UP

SEND OUT NEWSLETTERS, REMINDERS, AND MICRO-TRAININGS ALL YEAR LONG TO HELP PEOPLE REMEMBER WHAT THEY LEARNED.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

ACCESS CONTROL AND PRIVILEGE MANAGEMENT

THINGS TO DO

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE (POLP)

GIVE PEOPLE ONLY THE ACCESS THEY NEED TO DO THEIR JOBS AND NOTHING MORE. THIS MAKES THE ATTACK SURFACE SMALLER AND LESS LIKELY TO HAPPEN.

USE ROLE-BASED ACCESS CONTROL (RBAC)

LET PEOPLE GET TO ITEMS BASED ON THEIR JOB ROLES. THIS MAKES IT SIMPLE TO RUN AND MAKES SURE THAT ALL DEPARTMENTS FOLLOW THE SAME RULES.

AUTOMATE ACCESS REVIEWS

SET UP REGULAR CHECKS TO MAKE SURE THAT PEOPLE STILL REQUIRE THE ACCESS THEY HAVE BEEN GIVEN.

USE JUST-IN-TIME (JIT) PRIVILEGE ELEVATION

GIVE PEOPLE HIGHER ACCESS JUST WHEN THEY NEED IT AND TAKE IT AWAY AUTOMATICALLY WHEN THE JOB IS DONE.

CHECK ACCESS OFTEN AND KEEP AN EYE ON IT

WRITE DOWN WHO ACCESSED WHAT, WHEN, AND HOW. USE LOGS AND ALERTS TO FIND ACTS AND BEHAVIOURS THAT ARE OUT OF THE ORDINARY AND AGAINST THE RULES.

CENTRALIZE IDENTITY MANAGEMENT

USE IAM TOOLS TO KEEP TRACK OF IDENTITIES ON ALL SYSTEMS. THIS MAKES THINGS CLEARER AND EASIER TO UNDERSTAND.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

ACCESS CONTROL AND PRIVILEGE MANAGEMENT

DON'T DO IT!

DON'T GIVE USERS BROAD OR PERMANENT ADMIN ACCESS

GIVING USERS UNCONTROLLED OR LONG-TERM ELEVATED PRIVILEGES IS A BIG SECURITY RISK.

DON'T RELY ON DEFAULT SETTINGS

THE DEFAULT SETTINGS FOR ACCESS ARE TYPICALLY TOO PERMISSIVE. CHECK TO SEE IF THEY MEET YOUR SECURITY DEMANDS.

DON'T SKIP ACCESS REVIEWS

IF YOU DON'T CHECK ACCESS OFTEN, YOU CAN MISS SECURITY HOLES AND LET PRIVILEGE CREEP IN.

DON'T WAIT TO REVOKE

IF SOMEONE NO LONGER NEEDS ACCESS, TAKE IT AWAY RIGHT AWAY, ESPECIALLY IF THEY HAVE SPECIAL PRIVILEGES.

DON'T IGNORE ORPHANED ACCOUNTS

TAKE AWAY ACCESS FROM PERSONS WHO HAVE LEFT THE COMPANY OR SWITCHED JOBS. IT'S SIMPLE TO GET INTO ACCOUNTS THAT PEOPLE DON'T REMEMBER.

DON'T FORGET ABOUT THIRD-PARTY ACCESS

VENDORS AND CONTRACTORS SHOULD HAVE THE SAME TIGHT CONTROLS AS INTERNAL USERS.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

ASSET MANAGEMENT

THINGS TO DO

KEEP A CENTRALIZED INVENTORY

USE A SINGLE SYSTEM OR ASSET MANAGEMENT APPLICATION TO KEEP TRACK OF ALL YOUR ASSETS, INCLUDING HARDWARE, SOFTWARE, CLOUD RESOURCES, AND MOBILE DEVICES. THIS WAY, YOU CAN SEE AND MANAGE ALL OF THEM.

CLASSIFY ASSETS BY RISK AND CRITICALITY

FIND OUT WHICH ASSETS ARE NECESSARY FOR THE TASK AT HAND OR INCLUDE PRIVATE INFORMATION, AND MAKE SURE THEY ARE THE FIRST ONES TO BE PROTECTED.

AUTOMATE DISCOVERY & MONITORING

USE TOOLS TO FIND NEW ASSETS AND KEEP AN EYE ON CHANGES IN REAL TIME SO YOU DON'T MISS ANYTHING.

USE SECURITY TOOLS

CONNECT YOUR ASSET DATA TO SIEM, VULNERABILITY SCANNERS, AND PATCH MANAGEMENT SYSTEMS TO PROTECT YOUR ASSETS BEFORE THEY ARE ATTACKED.

INCLUDE SHADOW IT IN ASSESSMENTS

LOOK FOR DEVICES AND APPS THAT AREN'T APPROVED OR MANAGED AND COULD GET AROUND SECURITY CONTROLS.

CLEARLY TAG AND LABEL ASSETS

GIVE EACH ASSET A UNIQUE ID SO YOU CAN EASILY KEEP TRACK OF IT, CHECK IT, AND MANAGE ITS LIFE CYCLE.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

NABARD

DON'T FORGET ABOUT END-OF-LIFE ASSETS

ASSETS THAT ARE NO LONGER SUPPORTED OR HAVE BEEN RETIRED MIGHT STILL BE DANGEROUS IF THEY AREN'T PROPERLY DISPOSED OF OR ERASED.

DON'T KEEP TRACK MANUALLY

IT'S SIMPLE TO MAKE MISTAKES WITH SPREADSHEETS AND AD HOC LISTS, AND THEY GET OUT OF DATE QUICKLY. AUTOMATE WHENEVER YOU CAN.

DON'T DELAY ASSET UPDATE

HACKERS PREFER TO GO AFTER DEVICES THAT HAVE OLD FIRMWARE OR AREN'T PATCHED.

ASSET MANAGEMENT

DON'T DO IT!

DON'T FORGET ABOUT MOBILE AND REMOTE ASSETS

YOUR INVENTORY OF ASSETS SHOULD INCLUDE LAPTOPS, PHONES, AND CLOUD INSTANCES, ESPECIALLY BECAUSE MORE PEOPLE ARE WORKING FROM HOME.

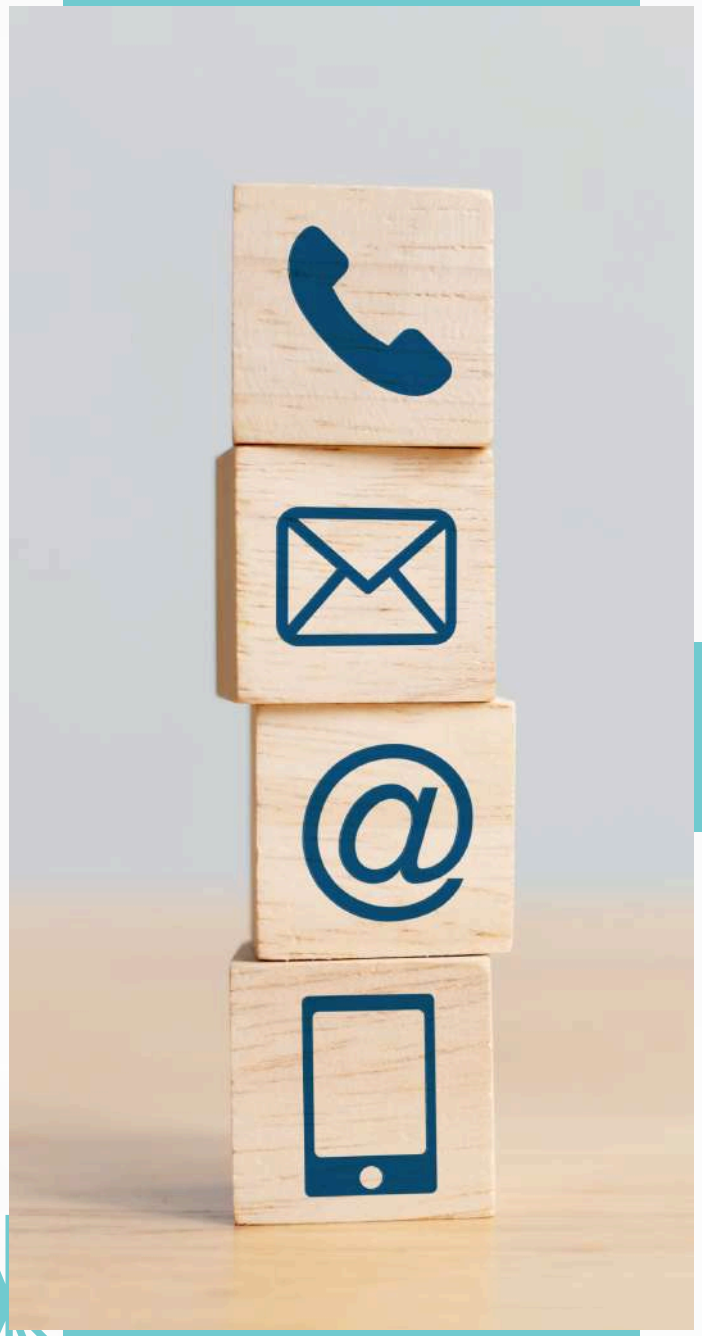
DON'T LET UNMANAGED DEVICES CONNECT TO THE NETWORK

EVERY DEVICE SHOULD BE EXAMINED, WATCHED, AND FOLLOW THE RULES.

DON'T TREAT ALL ASSETS EQUALLY

NOT ALL ASSETS NEED THE SAME LEVEL OF SECURITY. PUT YOUR RESOURCES WHERE THEY WILL BE MOST HELPFUL.

NATIONAL CYBERCRIME HELPLINE NUMBER 1930



FOR MORE INFORMATION

Contact us

NABARD

csite@nabard.org

Department of Supervision, 4th Floor, NABARD Head Office

022-2653 9028/ 9250/ 9484/ 9163

2025

International Year
of Cooperatives

NABARD

नाबार्ड
शब्द संपदा
वर्ष 2025

/nabardonline