

USE OF PUBLICLY OWNED IT RESOURCES POLICY

Effective	July 17, 2006
Purpose	To set forth departmental policy to ensure uniformity and consistency in the use and security of ODNR Information Technology Resources
Authority	Statewide Information Technology Policy DAS ITP-B.1, 2, 4, 5, 6 DAS ITP-D.4 DAS ITP-E.8 ORC 2909.04-5, 2913.04, 2921.41
Resource	Office of Information Technology

Computer hardware, software, and software services are publicly owned assets and are intended to be resources utilized by an employee in performing their job duties. Information contained on them is subject to review by department managers. As the user of IT resources, the employee will be held accountable for any misuse of the product.

Prohibited Uses of IT Resources

Any use of IT resources that is unlawful, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited and includes, but is not limited to, the following:

1. violating or encouraging the violation of local, state or federal law
2. downloading, duplicating, disseminating or printing of copyrighted materials such as texts, music and graphics
3. operating a business, directly or indirectly, for personal gain
4. accessing or participating in any type of personal ads or services such as dating, matchmaking, companion finding, pen pal or escort services
5. downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit materials
6. downloading, displaying, transmitting, duplicating, storing, or printing material that is offensive, obscene, threatening or harassing
7. organizing, wagering on, participating in or observing any type of gambling event or activity
8. sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk
9. except for agency approved efforts, soliciting money or support of behalf of charities, religious entities or political causes
10. impeding the state's ability to access, inspect and monitor IT resources. No employee or approved contractor shall encrypt or conceal the contents of any file or electronic communications or set or manipulate a password on any state computer, program, file or electronic communication without proper authorization from the Office of Information Technology
11. personal use of IT resources that disrupts or interferes with state business or incurs an

undue cost to the state

Hardware

Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any state-provided IT resource, including computers or network services, without prior authorization from the Office of Information Technology is strictly prohibited

Owner Responsibilities

The responsibility to adhere to federal copyright laws and proper licensing and distribution of the software and/or software services belongs to the "owner" of a specific software product and/or service. Responsibility is assigned as follows:

1. The Office of Information Technology is responsible for all IT products and services that have been procured by the Office for agency employees to perform their job duties.
2. The division/office is responsible for all products and services that have been procured by a division/office for employees to perform their job duties.
3. The employee is responsible for all products and services that have been procured by the employee to perform their job duties. In this particular case, the employee shall secure a waiver authorizing the use of the product and/or service signed by the division/office or Department representative and kept in the employee's personnel file. The waiver is intended to protect the employee as well as the division/office or Department.

Security and Confidentiality of Data Files and Safeguarding State Assets

All of the following activities are strictly prohibited:

1. Make or permit unauthorized use of any information in files maintained by the Department/Division/Office.
2. Seek to benefit personally or permit others to benefit personally by any information which has come to the employee by virtue of a work assignment.
3. Knowingly include or cause to be included in any record or report a false, inaccurate or misleading entry.
4. Remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of an employee's duties.
5. Use IT resources to violate or attempt to circumvent confidentiality procedures.
6. Accessing or disseminating confidential information about another person without authorization.
7. Accessing networks, files or systems or an account of another person without proper authorization.
8. Assist another to violate any part of this Code.
- 9.

Software Use and Duplication

The following points are to be followed to comply with software license agreements:

1. All software will be used in accordance with its license agreement.
2. No user will make any unauthorized copies of any software. Anyone found copying software other than for backup purposes may be subject to disciplinary action.
3. Acquisition and registration of shareware products will be handled in accordance with its license agreement. Shareware software is copyrighted software that is distributed freely through bulletin boards, web pages and online services.
4. Evaluation and Beta test copies of software will be used only for the time period agreed to in accordance with its license agreement.
5. Installing or using software including, but not limited to, instant messaging clients, video games (both stand alone and on-line), peer-to-peer file sharing software, or personally owned software on department-owned IT resources is prohibited unless approved in writing by the Office of Information Technology.
6. The "owner" shall follow the "one software package/one IT resource" rule when purchasing software. An equivalent number of software packages shall be purchased for every resource upon which it is run. With regard to use on wide or local area networks, or on multiple machines, owners shall acquire and use the software in accordance with the license agreement.

Privacy

Department IT resources belong to the State. Users should be aware that any files or communications made by or through State equipment may be subject to review by the department. The department may examine, monitor, search or disclose the contents of the files, including but not limited to e-mails, log files, data files, websites or calendars, at its discretion at any time.

Penalties

Violation this policy may result in disciplinary action or contractual penalties, and may be cause for termination. Additionally, the Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- 2909.04 using IT resources to disrupt or impair a government entity
- 2909.05 using IT resources to cause serious physical harm to government property
- 2913.04 accessing IT resources without consent of the owner
- 2921.41 using a public office to commit theft which includes fraud and unauthorized use of government IT resources

Anyone who becomes aware of a violation of these Codes shall report it to his/her supervisor or the violator's supervisor immediately. The Supervisor is responsible for notifying the Office of

Information Technology chief or assistant chief.

Glossary

1. **IT resources:** includes computers, servers, personal digital assistants, printers, copiers, fax machines, plotters, hubs, switches, routers, bridges, wireless access points, network interface cards or firewalls
2. **Owner:** the individual or organization that has legal right of possession or access to a specific software product and/or service. In the case of ODNR, the owner may be the Department, a division/office, or an employee, depending on who procured the product or service

INTERNET/INTRANET SECURITY AND USE POLICY

Effective	July 17, 2006
Purpose	To set forth departmental policy to ensure the integrity and security of the Department's Internet/Intranet System, and the uniformity and consistency of Internet use on ODNR's IT resources
Authority	Statewide Information Technology Policy DAS ITP-B.6 DAS ITP-E.8
Reference	Use of Publicly Owned Computer Hardware, Software and Software Services Policy
Resource	Office of Information Technology

ODNR employees shall not use the Department's Internet and Intranet servers in such a way as to impair the integrity and security of the systems. Nor shall employees use departmental computer hardware to access the Internet in a manner that interferes with business activities or is in violation of responsibilities outlined below. As the user of department's Internet/Intranet services, the employee will be held accountable for any misuse of these services.

Internet/Intranet Server Use

1. **All materials and applications to be posted to the Department Internet or Intranet servers will be tested on the web development server before deployment.** Web materials and applications must not compromise the performance, integrity and security of the Department Internet and Intranet servers. All materials and applications posted to the Department Internet or Intranet servers must also reside on the development server.
2. **Only authorized DNR staff may post materials and applications to the Department Internet or Intranet servers.** Each division and office shall authorize specific staff members to post materials and applications to the Department Internet or Intranet servers. These people will be responsible and accountable for the content of their division's web pages and the pages' impact on the Department's web site.

User Responsibilities

1. **Non-business uses of the Internet that interfere with business activities are not permitted.** Internet access is intended for official DNR business purposes. Personal use of the Internet that disrupts or interferes with state business, incurs an undue cost to the state, could potentially embarrass the state or has the appearance of impropriety is strictly prohibited.
2. **Using state IT resources for private business activities, sending chain letters, or soliciting money or support on behalf of charities, religious entities or political**

- causes is prohibited.** IT resources may be used to support department sponsored charitable events. Non-state employees may use state owned PC's that are designated for public use to access ODNR information that benefits a private business.
3. **Internet communications shall not contain offensive, obscene, threatening, harassing or incendiary statements.** Statements that disparage others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs as well as statements that promote violence or the use of weapons or devices associated with terrorist activities are strictly forbidden.
 4. **Sending, soliciting, viewing or downloading sexually oriented messages or images is strictly forbidden.**
 5. **Sending, soliciting, viewing or downloading messages or images that promote violence or are associated with terrorist activities is strictly forbidden.**
 6. **Disseminating or printing of copyrighted materials (including articles and software) in violation of copyright laws is prohibited.**
 7. **Users shall not provide unauthorized access to confidential information via the Internet.** All use of the Internet must be done in compliance with the rules and regulations that apply to such information. All reasonable means shall be employed to prevent the inadvertent dissemination of another person's private and/or confidential information via the Internet.
 8. **Use of another's account or signature line by a user is prohibited.** This includes all activities on the Internet (e.g., electronic mail or bulletin board system).
 9. **Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is prohibited.**
 10. **Users are prohibited from disabling anti-virus software or disseminating malicious code and are required to check all files downloaded from the Internet for malicious code (e.g., a virus), and shall report any incidents to the Office of Information Technology.** Users are required to utilize anti-virus software to check all files for code that could harm department equipment or systems by downloading them to disk. Users must report any malicious code detected to the OIT Support Desk (265-7082).
 11. **Unauthorized operation of, participation in, or contribution to an online community including, but not limited to, forums, chat rooms, blogs, wikis, peer-to-peer file sharing, social networks and non-work related , listservs is prohibited. Using an ODNR e-mail address on personal communications in online communities is prohibited.** Users can request approval to participate in these forms of communication if required for official business by contacting the Office of Information Technology.
 12. **Accessing or participating in any type of personal ads or services such as dating, matchmaking, companion finding, pen pal or escort services is prohibited.**
 13. **Organizing, wagering on, participating in or observing any type of gambling event or activity is prohibited.**
 14. **Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk is prohibited.**
 15. **Accessing Internet Service Providers for any purposes using the Department's network Internet connection is prohibited.** Users are not permitted to access personal e-mail accounts e.g., Hotmail.com, using a networked PC.

Penalties

Violation this policy may result in disciplinary action or contractual penalties, and may be cause for termination. Additionally, the Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- 2909.04 using IT resources to disrupt or impair a government entity
- 2909.05 using IT resources to cause serious physical harm to government property
- 2913.04 accessing IT resources without consent of the owner
- 2921.41 using a public office to commit theft which includes fraud and unauthorized use of government IT resources

Anyone who becomes aware of a violation of these Codes shall report it to his/her supervisor or the violator's supervisor immediately. The Supervisor is responsible for notifying the Office of Information Technology chief or assistant chief.

Glossary

1. **Internet:** A worldwide system of computer networks; a network of networks in which users at a computer can get information form another computer. The Internet is generally considered to be public, untrusted, and outside the boundary of the state of Ohio enterprise network.
2. **Intranet:** An Intranet is a private network that is contained within an enterprise. In general, an Intranet looks like a private version of the Internet. The main purpose of an intranet is to share enterprise information and computing resources among employees.
3. **IT Resources:** includes computers, servers, personal digital assistants, printers, copiers, fax machines, plotters, hubs, switches, routers, bridges, wireless access points, network interface cards or firewalls
4. **Malicious Code:** Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposed, without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

Hall, Nick

From: McCurdy, Charlotte
Sent: Wednesday, December 21, 2011 11:50 AM
To: Hall, Nick
Subject: Quail Hollow residenceuail
Attachments: Copy of residence tenant data sheet.xls

Nick,

I have attached the residence tenant data sheet document with my name typed into the form in the manager signature line and today's date. Please let me know if you need me to complete anything else on this form.

Charlotte

Charlotte McCurdy: District Preserve Manager
Ohio Department of Natural Resources
Quail Hollow State Park
13480 Congress Lake Avenue
Hartville, OH 44632
Office (330) 877-6652

OHIO DEPARTMENT OF NATURAL RESOURCES
OFFICE OF REAL ESTATE
RESIDENCE TENANT DATA SHEET

DATE 12/21/2011 AREA NAME Quail Hollow STRUCTURE NO. Levitt House

MAILING ADDRESS: 13344 Congress Lake Ave DIVISION: Parks & Recreation
Hartville, Ohio 44632-0823

PRESENT OCCUPANT:

NAME _____ DATE OCCUPANT WILL MOVE OUT _____

NEW OCCUPANT:

NAME Brad Dobney DATE OCCUPANT WILL MOVE IN 10-Dec-11

SOCIAL SECURITY NO. _____ JOB CLASSIFICATION Park Officer

OFFICE IN RESIDENCE No

UTILITY, SUBSIDY:

12/21/2011
DATE

Charlotte McCurdy
PARK MANAGER

12/22/11
DATE

[Signature]
ADMINISTRATOR

12.22.11
DATE

[Signature]
CHIEF, DIVISION OF PARKS AND RECREATION

Retain copy at PARK and Division Headquarters and forward original through channels to the Office of Real Estate.

MARKET RENTAL VALUE RENT
30% of Market Rental Value

From: Dobney, Brad
Sent: Wednesday, August 15, 2012 10:10 PM
To: 'brad.dobney@[REDACTED]'
Attachments: Five Things No One Tells You About Running.docx

Four Things No One Tells You About Running

Still possessed with plenty of free time and a relatively active mind (for now) I've decided to compile a list of things that no one tells about getting ready to run a race. This is half Cracked, half serious, and most of what I have to show for a day of work. All of my races save one have been half marathons, so most of this is taken from those four massive training efforts I have made. Since I started training for the first race I was in (a relay in Akron) I've logged about 1,400 miles in the pursuit of something. This is what I've learned.

It Hurts: Lots of things hurt: getting kicked in junk, breaking bones, stubbing your toe, or just sitting in one place for too long. None of those comes with the added bonus of being completely self-inflicted. Running hurts, and no one does it to you but you. As an added bonus, running hurts in ways that you didn't think were possible. A good ten miles can reduce you from a strapping athlete with the boyish good looks of Jude Law, to feeling like David Spade when Chris Farley's bed collapses on him. As you near the end of those ten miles, your quads will hurt, your hamstrings will hurt, your feet will hurt, and even your shoulders will hurt. Rather than take this as a sign that you should quit this insanity, you'll contemplate whether you can push another mile out. As you lay on the couch that night, barely able to feed yourself, your wife will almost question all the decisions she made that led her to be anywhere near this quivering, groaning, uncontrollably flatulating husk of a man.

It destroys your body: Pain at the time isn't the only thing you have to look forward to though, you young imitator of Mercury. From the moment you start running as a hobby or training for a race until (I assume) the moment you die, you will never bounce out of bed again. You won't really bounce anywhere again. See, all that pounding and all those miles will be the inevitable process of turning your joints into something that feel like a lovely combination of mulch and gravel. Your knees stiffen up when you sit down, your back seizes up at the very mention of the word "hill", and muscles that sat dormant in your legs for the previous twenty years first swell, then just ache. It's not all lower body either. Keeping your arms pumping away as if you are the pole for over ten miles causes neck and shoulder soreness that doesn't just go away. And you might as well take a cheese grater to your nipples, because the sweat soaking your shirt turns it into some sort of fabric monster bent on areola destruction. On top of all that, your feet will literally disintegrate to the point that you consider Adam Walker the paragon of podiatry health. Of course, all that assumes that you don't suffer some sort of serious injury while running that prevents you from running.

It takes a lot of stuff: If you thought that all you need to run was your feet and some open space, you are wrong (and also probably a hipster, get that checked). For starters, you need shoes. Not just any shoes either, you need running shoes. They need to weigh a small enough amount that discussing them sounds like a drug transaction, but still provide some cushion to slow the ruination of your joints. Then you need a watch. Again, not just any watch, but a watch that knows where you are, where you've been, and the time elapsed between those two points. You also may need: some shorts that don't weigh as much as basketball shorts, an mp3 player, more earphones for your mp3 player, because sweat destroys those things, tape for various injuries, and a copious amount of Vaseline.

It's addicting: After all that I have mentioned before it might seem like running is not something you would ever consider. Unfortunately, once you start, you can't stop. Running comes with some side effects that are not negative. For one, you'll lose weight at an amazing clip. This leads to being able to eat almost whatever you may care to, content in the knowledge you will run it off the next day. You'll also start to feel (more) superior to people who are not running at that very moment. Average sized people simply out walking you can now regard with a sneer, because you are a runner. Bikers are also lesser life forms, because they take the easy way out. They are Bear Grylls in a powered glider to your Sir Edmund Hilary and Tenzig Norgay. Why can you be two people in that analogy? Because you run, and you just can. Heaven forbid you come across someone who doesn't exercise at all. What does that lump of flesh have to offer you? Nothing, that's what. They've never set out to conquer new lands (or just a Giant Eagle parking lot) with nothing but their own two feet and the resolve that made America great. No, they know nothing about success in cold so pervasive it freezes your knob or heat so bad it throws your body chemistry off. You are a great American, they just work at Taco Bell or something like that.

That all pales in the face of the greatest addiction of all though, watching the mile count rise. Doing something is nice. Doing something you can quantify with a hard number, a chart, and a bar graph is way, way better. It really is difficult to explain how fulfilling it can be to watch that next round number come into view and then slowly fall behind you. Just typing it "400 miles down" feels like a vindication of every step it took to get there. It's that little pull that forces you out on a Monday to make May a 60 mile month instead of a 57 mile one. Perhaps even better than that is moment in a race when you pull even with someone you have chased for a mile or so. You both know where you have been and where you are going, it's just a test to see who gets there first. The fact that you are both in your late 20s and well past any sort of competition that matters is of no concern. It's just you and him, and passing him and putting him away is a feeling that is difficult to forget.

Exhibit 4

Page 4 of 5

From: Dobney, Brad
Sent: Wednesday, August 29, 2012 10:28 PM
To: brad.dobney@[REDACTED]
Attachments: Article.docx

A game at the Cintas Center used to be one of the highlights of the year for Joel (the other moderator of Banners) and I. As we both chose to pursue our dreams of playing college sports at a level more befitting our talent, we didn't have the opportunity to attend Xavier University. When we got the chance to attend a game then, it was an event. Something about walking in to the Cintas and seeing people doing the same thing that we did, but on a grander scale, produced goosebumps every time. Even now, from media row, it's difficult not to get sucked in to the spectacle that is a Xavier basketball game.

This originally started as an article about our favorite parts of the gameday experience. Unfortunately, the debacle of the last week has drained a bit of the impetus from that idea. Seeing this draft sitting here got me to thinking though. What will a game at Xavier be like now? Dez Wells is gone, The Fight is still fresh in the minds of everyone making decisions, and there is an unease surrounding the program right now.

Still, a game will surely still be a good time, won't it? The key elements are still there. Xavier basketball will always be my first love, and no amount of off court turmoil will change that. The atmosphere from the student section will still be unmatched anywhere this side of Utah State, there is a reason that the Cintas Center is one of the most difficult road venues in the nation. Production will still be top notch. Brian Hicks, Tom Eiser, and dozens of other people that no one ever sees work tirelessly to make sure that no one attends a Xavier game and walks away feeling like something was missing. Really, nothing ever is.

So why am I having such a hard time getting excited right now? Maybe I'm afraid that Dec 10 did change something. That the fans will be just that little bit more on edge, not wanting to be the people hammered for sparking off another incident. Maybe I'm just bummed that I won't get to see Dezmine Wells develop in person. I've not been that excited for a Xavier sophomore in a very long time. More than his talent, maybe I'm just going to miss the spirit with which he played the game, my game. Maybe I'm afraid that Xavier just won't be that good this year. Maybe I'm worried that some tiny part of me isn't excited because I know there isn't anything to be excited about.

Last year, when I walked in the tunnel hours early, Kenny Frease was the only player on the court. I stood there for a long time and just watched him shoot free throws. Each miss prompted a grimace, consecutive misses prompted a bit more. Occasionally the ball bounced away and I would tap it back to the big man. Neither of us said anything, we just stood there, one shooting, one watching. On that day, there was nowhere I would rather have been. Maybe I'm not excited because I'm not sure I can say that anymore. Maybe I'm not excited because a little piece of me, a little piece of that kid who loved nothing more than watching his favorite team live on gameday, finally had to grow up. Maybe I'm not excited because part of what made Xavier so unique, so amazing on those special days, just died. Maybe we're all afraid that this is the end.

VOICE RADIO & MOBILE DATA COMMUNICATIONS DIRECTIVE

Effective	November 1, 2009
Purpose	To establish standards of operation for ODNR “Field User” voice radio & mobile data communication. This shall apply to all ODNR Divisions, Offices, and agreement holders that operate or use ODNR 700-800mghz radios on the Multi Agency Radio Communications System or similar systems operated by another agency
Authority	Federal Communications Commission Rules and Regulations: 47CFR80 – Maritime Radio Services and 47CFR90 – Private Land Mobile Radio Services – Ohio LEADS Rules and Regulations – DAS-OIT- MARCS Office Rules, ODNR Office of the Director-MARCS/Legacy Radio Equipment Acquisition, Repair, Installation & Use directive. DAS Policy ITP-B-3.
Reference	FCC Rules and Regulations DAS Policy MPM15 Interoperability Talkgroups Ohio LEADS Rules DAS Policy ITP-B-3ODNR Law/Admin-Maint. Field Subscriber Training Manuals
Resource	Office of Law Enforcement, Chief Staff Officer for Training ODNR Comm. Center LEADS TAC

ODNR Officers shall adhere to the following Directive when using ODNR voice radios and mobile data.

RADIO/MCT USAGE OVERVIEW:

1. The ODNR-MARCS radio system is a “Trunked” radio system that enhances radio interoperability between agencies that have access to statewide Interoperable Talkgroups. Participant agencies share the same communications infrastructure when communicating on an agency specific Talkgroup, or with another agency on an Interoperable Talkgroup. ODNR voice radio and data users must remember that use of the MARCS infrastructure affects both ODNR users and other agencies alike.
2. “Use of ODNR-MARCS by ODNR Field Users must be related to business operations of ODNR and/or within the scope of the Field Users duties.
3. ODNR radio communications may be a public record. The use of obscene, profane, threatening, derogatory, racist, gratuitous, sexually explicit or suggestive language on any ODNR, MARCS Talkgroups, channels or through the use of mobile data is prohibited by this directive and Federal Communications Commission rules.
4. All ODNR employees issued ODNR communications equipment are required to attend standardized training, developed by or endorsed by the ODNR Office of Law

Enforcement. Use of equipment will mirror the training received and follow the user handbook received during training. In the absence of policy, procedure or directive, training will set the standard for equipment use.

5. Effective radio communications requires a balance of professionalism, competency, and familiarization when obtaining or relaying complete and accurate information through radio and mobile data. Employees who consistently use the system to its maximum capability will benefit from improved crime and problem solving.
6. During critical incidents, employees will experience mental and physical forces that may affect the nature of their communications. Persons in stressful situations will revert to their training. Subsequently it is vital that radio users train routinely with critical incidents in mind.

Voice Radio Communication Procedure:

The following procedures will be used when ODNR field users are conducting voice communications;

Hailing the ODNR Comm. Center, another employee or facility:

1. Identify the person you are calling by radio unit number.
2. Identify yourself by your assigned radio unit number.
3. Identify the Talkgroup that you are transmitting on.
4. Declare if you are transmitting in un-encrypted mode.
5. Wait for the Comm. Center/Field User or Facility to respond.

Do not state the reason for your traffic without allowing the Comm. Center/Field User or Facility to respond, acknowledging your call first.

An example of proper traffic:

1. "Columbus from 9912 call south west."
2. "Go ahead 9912, this is Columbus."
3. 9912 then proceeds to give a message to the Comm. Center or field user or facility.
4. Once the communications are completed, the initiating unit (9912) concludes the communication by stating
"9912 clear on call south west"

The following are exceptions to this rule:

1. Officers operating on an encrypted talkgroup and calling the ODNR Communication Center need not declare Secure or Clear.
2. Officers operating on an encrypted talkgroup & calling the ODNR Communications Center with signal 7, 11, 86 or CCH;
3. May declare the purpose but not the content of their traffic, without waiting on the

Communications Center to respond. i.e., “Columbus from 9912, Call SW, signal 7”

Transmitting Encrypted:

1. Law enforcement radios will be kept in encrypted mode until such time clear non-encrypted transmission is required. Once the unencrypted transmission is concluded, the radio will be returned to an encrypted condition.
2. All LEADS transmission and sharing of LEADS generated data will be transmitted/received on encrypted Talkgroups only.
3. Intel generated from homeland security sources, Maglocen type databases, or ODNR internal databases will only be transmitted/received on encrypted talkgroups.
4. An exception to the encryption rule would be permissible, only if temporary sharing of information is required on interoperability or unencrypted Agency Specific Talkgroups, and is authorized by a supervisor or Incident Command or by employees with non-encrypted radios with emergency traffic. Officers, supervisors and incident commanders should be able to articulate the need and justification for such sharing of information over non-encrypted Talkgroups.

Buckeye State Sheriffs Codes, & NIMS:

1. When communicating your status or disposition to the ODNR Comm. Center, a field user or facility, ODNR Field Users are encouraged to use BSSA codes and signals. Use of plain language is permissible when codes are not known.
2. Plain language will be used when communicating with other agencies and agencies involved in NIMS-emergency incidents or joint-operations.

LEADS & NCIC Rules:

All LEADS & NCIC rules, & Ohio Administrative Rules, including but not limited to; proper dissemination & record keeping, jurisdiction, justification & training, will be followed and adhered to by all ODNR users.

Vehicular/Fixed Repeaters:

Vehicle repeaters will be turned on & kept in the mobile mode until needed by the portable radio user. Continued practice and use of the VRS-FRS is vital for operational success. Officers and employees should routinely use the VRS-FRS to maintain proficiency or familiarization in the event it is needed.

Voice radio Talkgroups:

Voice radio Talkgroups are designated for specific purposes:

ODNR Agency Specific Talkgroups:

The ODNR Communications Center routinely monitors the following Talkgroups;

Exhibit 5

1. CALL-xx (CALLCEN, CALLSE, etc.)
2. xxx-DNR (CENDNR, SEDNR, etc)
3. Emergency
4. SO regional Call Talkgroups. (SOSE, SOCEN, etc.)
5. MCALL 1-4

**ODNR Agency Specific Talkgroups described:
The following are encrypted talkgroups**

CALL-xx:	Call Talkgroups. This talkgroup will be used to establish communications with another field user, the Comm. Center or a facility. Once communications are established, radio traffic will move to a Division specific Talkgroup, i.e.; WLD4E, PR-R08-E, PR-R16-M, WCE-AKRON, etc. The Comm. Center will usually direct field users to xxxDNR. Field Users will avoid tying up this Talkgroup with routine traffic between Field Users
xxx-DNR:	Communications Talkgroup. The ODNR Comm. Center will direct users to this Talkgroup to receive traffic. Field Users will avoid tying up this Talkgroup with routine traffic between Field Users.
DNR-TAC:	Tactical Talkgroup. Law enforcement operations-projects other than routine patrol.
EMERG:	For Field Users communicating after the emergency button has been pushed.
DNR-IC:	Incident Command for ODNR exempt employees or designated field users.
FR-ENF-X:	Routine law enforcement operations-projects for forestry officers in the north or south region.
FR-XXX-M:	Forestry admin./maint. operations for a specific region office.
FR-FIREX:	Fire line operations.
PR-RXX-E:	Routine law enforcement operations for park officers in a specific park region.
PR-TAC-X:	Special law enforcement operations-projects for park officers in a north or south region.
PR-SPL-X:	Special event communications in the north or south region for park employees.
PR-RXX-M:	Park admin/maint operations for a specific region office.
WCE-XXX:	Routine law enforcement operations-projects for watercraft officers in specific

	regions
WL-DX-E:	Routine law enforcement operations-projects for wildlife officers in specific regions.
WL-DX-A:	Special law enforcement operation/projects for wildlife officers.
WL-DX-B:	Special law enforcement operation/projects for wildlife officers.
WL-DISTX:	Administrative or events relating to specific wildlife districts.
NAP-X:	Routine law enforcement operations-projects for natural areas officers in north, south, & central region.
MRM-X:	Mineral resources operations in the north, south, west regions.
MRM-EMER:	Mineral Resources Emergency response teams.
NR-RSVXX:	Inactive. Reserved for DNR use.
Interoperable Talkgroups described: (Non encrypted talk groups)	
800 MHz interoperable channels with police, fire, homeland, federal agencies	
8ICALL	NPSPAC Hailing channel on select urban towers
8ICALLTA	NPSPAC Hailing channel Talk Around off tower
8ITAC-X	NPSPAC TAC channel on select urban towers
8ITACTA	NPSPAC TAC channel Talk Around
AIRMDX	Medical Transport Aircraft – life flight analog 800mgz
TA-X	Talk around 800mgz
Ohio Interoperability Talkgroups: (Non encrypted talk groups)	
MCALLX:	Hailing all MARCS users, All MARCS agencies.
MCOMMXX:	Communications Talkgroup for all MARCS Agencies.

Exhibit 5

ECOMM XX:	Emergency operations channels for use during coordinated emergency response with Ohio EMA and other agencies.
CMD0X:	ODNR command Talkgroup for use during ECOMM responses.
NR-COMX:	ODNR command Talkgroup for use ECOMM responses.
NR-ALL:	ODNR Announcement Talkgroup for ECOMM responses.
HELPDESK:	Talkgroup for access to the DAS MARCS Helpdesk.
SCALL:	Transportable communication system hailing Talkgroup.
SCOMM0X:	Transportable communication system communication Talkgroup.
SCMD0X:	Transportable communication system Command Talkgroup.
SO-XX:	Regional hailing Talkgroup for Sheriffs Offices.
SO-00:	Specific sheriff's office Talkgroups by County number.
SO-00DISP	Specific sheriff's office dispatch Talkgroup by County number.
LEERN0XA-B:	LEERN TAC Talkgroup.
LEERN0X:	Regional LEERN Talkgroups.

Foreign Systems:

A Foreign System is best described as another agencies system parameters and talkgroups that are placed into an ODNR radio. Foreign system programming is permitted by the ODNR Office of Law Enforcement and the approving agency whose talkgroups will be placed into the ODNR radio. Field Users who have notified in writing ODNR Office of Law Enforcement of the Officer's name, work unit/facility and system name may take ODNR radios to the cooperating agency and receive programming:

1. Only in the personality, scan list, and zone/channel assignment location(s) allocated by ODNR Office of Law Enforcement.
2. Only if it does not alter the approved feature set for that radio.
3. Only if the contents of ODNR radio programming are not shared, accessed or retained by the cooperating agency or any person not authorized by the ODNR Office of Law Enforcement.
4. Only law enforcement voice equipment may be programmed with foreign systems.

5. The divisions will be responsible for coordinating with all foreign system administrators for the purpose of programming foreign systems into ODNR MARCS voice equipment.
6. The divisions will be responsible to ensure that any voice equipment which is going to be programmed by a foreign system administrator is fully operational.
7. The divisions will be responsible to ensure that any voice equipment which has been programmed by a foreign system administrator is fully operational.
8. The divisions will be responsible to repair and/or replace any ODNR voice equipment that is damaged or destroyed while in possession of any foreign system administrator.
9. The division will be responsible to guarantee that no foreign system administrator modifies the functionality and setup of ODNR templates and the hardware features. The foreign system administrators are only allowed to add their programming in the portables in zone 28 and higher and in the mobiles in zone 26 and higher. The divisions will be solely responsible for any and all funding required to complete any foreign system programming and repair if the voice equipment is damaged during this process.
10. Officers who choose to install a foreign system will not utilize the foreign system as their primary operational system on a permanent basis. The ODNR dispatch will be the primary dispatching system for ALL officers. Officers will not be able to scan a foreign system and may utilize their portable and mobile in conjunction to monitor both dispatch facilities. If an officer needs to exit their vehicle and elects to operate on the foreign system the officer will advise the ODNR dispatch of the location they are out at and the foreign system they are on if it is a non emergency situation and time allows. If the officer conducts a traffic stop or exits the vehicle in a emergency situation they will check back into the ODNR dispatch as soon as reasonably possible or request the foreign system dispatcher to advise the ODNR dispatch of their status. Officers are responsible for managing their communications capabilities with ODNR and the foreign system dispatchers by keeping them informed of status for officer safety during a dispatcher check-up. Unnecessary dispatcher initiated emergency response for "Officer in Trouble" due to a communications notification failure by the officer outside of an emergency situation is unacceptable.

Programming & Maintenance:

1. ODNR radio's, VRM's and any other device, program, template, feature set or hardware that relates to or is a part of the ODNR voice & mobile data system will be accessed, programmed, maintained, altered or repaired, only by persons approved by the ODNR Office of Law Enforcement. Exception section 8 par. 1.
2. Only talkgroups, frequencies, feature sets, programs, applications and configurations approved by the ODNR Office of Law Enforcement will be permitted in any ODNR radio, mobile data system and its related devices, programs and hardware.

Interaction with CAD:

Sign on and sign off and routine status updates are a vital link between the ODNR

Exhibit 5

Page 8 of 13

Communications Center and the Officer. The ODNR Communications Center is established to be the designated means through which ODNR officers are dispatched and information is relayed from the public and other agencies to ODNR officers and employees.

While beneficial in many aspects (including officer safety, crime solving, and emergency response), local agency dispatching will not be used to the exclusion of the ODNR Communications Center.

Sign in:

Law Enforcement:

Mobile Data: Mobile Data equipped Officers will sign on using the mobile data computer when beginning a work period and will keep mobile status updated for the duration of the work period. At a minimum, Mobile Data equipped Officers will use mobile data to update their status hourly and/or when their work status, facility, or geographical jurisdiction changes when the officers is in the vehicle or vessel. Officers who are mobile data equipped and sign on as voice only must contact the MARCS help desk for a trouble ticket. ODNR Comm. Center dispatchers will monitor voice only sign on to ensure data users are using the data equipment and any data equipment issues are identified and reported to MARCS. However, Mobile Data users who are going in-service for a period less than 30 minutes may advise the Comm. Center of voice only status without having to use the mobile data system.

During events of mobile data coverage outage, officers should sign on using the voice radio and advise the comm. center of coverage outage. Once Coverage becomes available, the officer will sign on using mobile data.

Voice Only: Voice only equipped officers will sign on using the voice radio when beginning a work period or when returning from a status that showed the officer unavailable. *“See Updating Status”*

Admin-Maint: Admin-Maint. users will notify their facility that they are using a radio and keep their facility updated on their status throughout the work period. Facilities will keep track of the radio and corresponding digital id that Admin-Maint employees are using in the event of an emergency initiation.

Admin-Maint. Users working at a time when their facility is closed may use the ODNR Comm. Center to sign in if they so desire. When calling the ODNR Comm. Center, declare that you are calling on an un-encrypted or “Clear” talkgroup.

Sign out:

Law Enforcement:

Mobile Data: Mobile Data equipped Officers will sign off using the mobile data computer when ending a work period. During events of mobile coverage outage, officers should request the Comm. Center sign them off using the voice radio. **Do not** sign off on voice & then sign off on

Mobile data. Doing so will result in an error in the CAD database that will effect your future ability to sign on and off.

Voice Only: Voice only equipped officers will sign off using the voice radio when ending a work period.

Admin-Maint: Admin-Maint. Users will notify their facility that they are ending use of the radio.

Admin-Maint. Users, working at a time when their facility is closed, may radio the ODNR Comm. Center to sign off.

Updating Status:

Law Enforcement:

Mobile Data: Mobile Data equipped Officers will use mobile data to update their status hourly and/or when their work status, facility, or geographical jurisdiction changes.

During events of mobile coverage outage, officers should update their status using the voice radio.

Voice Only: Voice only equipped officers will update their status when their work status, facility, or geographical jurisdiction changes.

Admin-Maint: Admin-Maint. users will keep their facility updated on their status throughout the work period. Facilities should keep track of the radio and corresponding digital id that Admin-Maint employees are using in the event of an emergency initiation.

CAD Emergency:

Certain buttons on the Portable Radio, Mobile Radio, and MCT enable the user to send an emergency signal when help is needed.

1. **Emergency Defined:** An emergency does not include items of a routine matter that law enforcement officials would encounter in their normal work cycle. It is the combination of circumstances calling for action to save or protect persons or property. An emergency is a combination of inherently dangerous situations that demand an immediate response, where the officer reasonably believes that there may be serious personal injury or significant property loss. Decision-making must be based upon the totality of the circumstances known at time to the officer, such as serious personal injury, proximity of other officers, seriousness of the offense or incident.
2. **Responding to Emergency:** All Officers hearing, observing or dispatched to assist another Officer that can reasonably offer assistance, will notify the ODNR Communication Center and proceed to the Officer(s) in need of assistance, unless; circumstances dictate you can not offer assistance at that time, a supervisor advises not to respond, or the

ODNR Communications Center advises otherwise.

3. Clearing an Emergency: Whether intentional (code 44) or unintentional (44i), once the emergency button has been pushed on a mobile, or portable radio, if able, the initiator will notify the Comm. Center of the nature of the emergency using voice communication.

Incident documentation:

ODNR Incident documentation will be NIBRS and OIBRS compliant. Incidents are defined as an event/violation/or offense/ or complaint that is governed by the ORC or Administrative Rule, or one that results in injury, death, property loss or damage.

*The following 2 paragraphs will be required upon the implementation of ODNR Field Based Reporting.

1. When an officer handles an incident they will self generate an incident number, or acquire an incident number from the ODNR Comm. Center. Incident numbers will link all events, work products, and records relating to an incident.
2. Incidents will be updated, and when completed, closed with the applicable status and disposition, and follow the stipulated workflow for each NIBRS document.

MCT Security:

1. Passwords & Usernames: User names, passwords, accounts and security tokens are established to provide security for computer networks, protect sensitive data and written communication and prohibit unauthorized access to devices used by field users

Usernames, passwords, account information and security tokens will not be shared, displayed, or made accessible to any person other than the person to whom that information has been issued.

The Exception to this rule will be, ODNR OIT helpdesk and technicians, as well as designated ODNR Office of Law Enforcement Staff may view and obtain passwords, usernames, and account information from the issued person, for the purpose of repairing or configuring accounts and devices.

2. Viewable Screen: MCT users will not permit unauthorized persons, persons without jurisdiction, or persons without applicable credentials to view on a computer monitor or screen, any data deemed sensitive or restricted by a Division, Office, or the ORC. This includes MCT's and computers that may be unattended and left on in a vehicle, vessel, command vehicle, command trailer or other facility or area under the control or use by ODNR employees.

Remedy Helpdesk:

1. Helpdesk cases: Employees experiencing problems with the ODNR radio communications or data equipment will contact the DAS MARCS helpdesk to initiate a

Helpdesk Case. Confirm your contact information is accurate. Keep the helpdesk case number for further reference. 1-866-OH-MARCS

2. Change request:

1. Change of position/New position/vehicle-vessel changes:

Notification of transfers, retirements, and new hires will be called into the OIT MARCS Helpdesk 614-265-7082 to initiate a Change Request.

Notification of transfers, retirements, and new hires will also be sent to the ODNR Comm. Center using the Comm. Center information forms.

Notification of vehicle-vessel changes will be called into the OIT MARCS Helpdesk to initiate a Change Request. Additionally, e-mail should be sent to ODNR Office of Law Enforcement and the related change request number referenced.

Position changes requiring new equipment will be called into the OIT MARCS Helpdesk and a Change Request will be initiated.

2. Lost or stolen equipment:

Immediately contact the ODNR Communications Center and report a stolen, lost device and contact the MARCS helpdesk to create a Help Desk Case and record the number. If the device has been stolen, initiate a critical incident notification.

Corrective Action:

Persons violating any element of this directive will be subject to progressive discipline as outlined in the State of Ohio employee discipline guidelines.

Glossary

Admin-Maint	An employee of ODNR who is not commissioned as an officer.
CAD	Computerized Dispatch consoles in the ODNR Comm. Center.
Change Request	A MARCS Helpdesk process that documents a requested change, deletion, or addition.
Clear	A radio transmitting without encryption.
Comm. Center	The ODNR Communications center and staff located at 2855 W. Dublin Granville Rd. Columbus.

Exhibit 5

Control Stations	Refers to a base station radio that resides at a facility, or mobile command vehicle.
DAS	Ohio Department of Administrative Services
Digital ID	The six digit id that is unique to each radio.
Emergency	An activation of the radio or MCT emergency button that results in an emergency incident in the ODNR CAD.
Encryption	Random algorithm program that makes law enforcement transmissions unreadable by a non-encrypted radio or scanner when the encryption function is activated.
FRS	Fixed Repeater System. A stationary repeater accessible to both commissioned and non-commissioned employees through their portable radio.
Feature Set	An ODNR pre-determined configuration of the radio that controls access to private call, and other enhancements and parameters established in ODNR Templates.
Field User	Any ODNR employee, volunteer or agreement holder using radios or mobile data for law enforcement, administrative, maintenance, education, research or incident command purposes, with the exception of the ODNR Communications Center.
Foreign System	A MARCS compatible system and talkgroups that belong to another agency that may be compatible with ODNR radios and data transmitting devices.
Help Desk Case	A MARCS helpdesk process that documents a problem with equipment or the MARCS system itself.
NIBRS	National Incident Based Reporting System
NIMS	National Incident Management System.
Law Enforcement	A commissioned officer of the State of Ohio or an Officer of the United States Gov. empowered with authority to enforce state local, or federal law.

MARCS	Multi Agency Radio Communications System
MCT	Mobile Computer Terminal.
OIBRS	Ohio Incident Based Reporting System
Secure	A radio transmitting encrypted
Talkgroups	A radio channel designed to be used by a specific group of Field Users and the ODNR Comm. Center.
Talkgroup, Agency Specific	Talkgroups designated to be used by a specific agency, or organizational unit. Agency Specific talkgroups can not be accessed by another agency.
Talkgroup, Interoperable	Talkgroups designated for use by all participating MARCS users, or users having access to interoperable talkgroups-channels.
Transportable Communications System	An ODNR, DPS, or BSSA vehicle capable of coordinating communications between multiple users and agencies. The TCS may also possess equipment, which allows it to operate as a stand-alone trunked radio site.
Trunked Radio System	A radio system allowing multiple users to access different channels on one tower site at the same time.
VRS	Vehicular Repeater System that is installed in all vehicles with mobile data. VRS is not installed in Vessels. VRS may also be installed at facilities as a fixed unit accessible through a tower site at the facility.
Unsecured	A radio transmitting unencrypted