# Cryptography

Version 12.0

Issued: 25th December, 2024

Document Owner: Information Security Manager



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

# 1 TABLE OF CONTENTS





Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

## 2 DOCUMENT CONTROL SHEET

| Document History | | | | Approval | |
|---|---|---|---|---|---|
| **Ver.** | **Date** | **Author** | **Comment** | **Date** | **By** |
| 0.1 | 25.11.2016 | *Marjan Sterjev* | Initial version created. | | |
| 0.2 | 28.11.2016 | *Zhaneta Ilievska* | Added additional sections: Terms and Definitions, Related documents | | |
| 1.0 | 11.05.2018 | *Marjan Sterjev* | Reviewed and added the File Servers Encryption section | 18.05.2018 | *Zhaneta Ilievska* |
| 2.0 | 19.12.2018 | *Zhaneta Ilievska* | Update upon review with ISC<br>-Added policy that encryption shall be applied to portable devices with Linux and iOS<br>-Added key terms in definitions and abbreviation<br>-Added related documents section | 19.12.2018 | *Zhaneta Ilievska* |
| 3.0 | 03.08.2019 | *Marjan Sterjev* | Added more cryptography related details related to SSL/TLS, SSH, Linux passwords. | 03.08.2019 | *Zhaneta Ilievska* |
| 4.0 | 19.11.2019 | *Marjan Kuzmanovski* | Added VPN server cryptography details | 20.11.2019 | *Zhaneta Ilievska* |
| 4.1 | 24.11.2020 | *Zhaneta Ilievska* | Non-substantial change - Removed next update | | |
| 5.0 | 24.11.2020 | *Marjan Sterjev* | Reviewed, Approved | 24.11.2020 | *Marjan Sterjev* |
| *6.0* | *12.01.2021* | *Zhaneta Ilievska* | Re-branding – logo, e-mail address changed in header/footer. | 12.01.2021 | *Marjan Sterjev* |
| 6.1 | 09.06.2021 | *Zlatko Chavdarovski* | Updated section “Mobile Device Encryption” - due to implementation of Microsoft Intune - all Windows workstations are enrolled in Microsoft Intune and drive encryption are checked near real-time by Microsoft Endpoint Manager | | |
| *7.0* | *30.09.2021* | *Zhaneta Ilievska* | Review, cosmetic changes, Added IW_IS_Policy as superior document, SP links to referenced documents | 30.09.2021 | *Marjan Sterjev* |
| 7.1 | 28.10.2021 | *Marjan Sterjev* | Removing SSL in the document. **Only TLS shall figure out**.<br>Introduced small notes about **Microsoft Intune that monitors the smart phone’s encryption status**.<br>In addition, a small note has been added that **sensitive e-mail messages can be sent encrypted by using Office 365 Message Encryption mechanism**. | | |
| *8.0* | *29.10.2021* | *Zhaneta Ilievska* | Review, Accepted changes | 28.10.2021 | *Marjan Sterjev* |
| *9.0* | *10.10.2022* | *Zhaneta Ilievska* | Changed location address in footer, no other substantial changes | 10.10.2022 | *Marjan Kuzmanovski* |
| 10.0 | 23.11.2022 | *Zlatko Chavdarovski* | Minor changes:<br>- 5.1 - Added Windows 11 as operating system installed on workstations<br>- 7 – Added LAN access for user authentication with certificates | | |
| 10.1 | 27.12.2022 | *Zlatko Chavdarovski* | Replaced ‘Office365’ with ‘Microsoft365’ throughout the document, since Microsoft officially renamed the subscription to ‘Microsoft365’ | | |
| 11.0 | 4.12.2023 | *Zlatko Chavdarovski* | Review, minor changes | 28.12.2023 | |
| 11.1 | 17.09.2024 | *Zlatko Chavdarovski* | -Updated wording throughout the document<br>-Local CA – compromised certificates are revoked<br>-Added section “Trusted Certification Authorities”<br>-Added section ”Roles and responsibilities”<br>-Added section “Encryption in Cloud services” | | |
| 12.0 | 25.12.2024 | *Zlatko Chavdarovski* | Date of issuing | 25.12.2024 | *Marjan Kuzmanovski* |

| Document summary | |
|---|---|
| **Document name** | IW_Cryptography |

| | |
|---|---|
| **Author and colaborators** | Marjan Sterjev, Marjan Kuzmanovski, Zlatko Chavdarovski |
| **Document owner / OU** | Information Security Manager |
| **Summary of the document** | Policy for using cryptography in the company to protect the information from unauthorized access |
| **Version** | 12.0 **Issued on date:** 25.12.2024 |
| **Application** | InterWorks |
| **Classification** | Internal |
| **Place of publication** | Intranet (Document Management System) - ISMS Site – Document Library |
| **Superior document** | IW_IS_Policy |

**Distribution**

| Version | Date | Location | Distribution list | Distributed by |
|---|---|---|---|---|
| 1.0 | 18.05.2018 | ISMS site | All Employees | Zhaneta Ilievska |
| 2.0 | 19.12.2018 | ISMS site | All Employees | Zhaneta Ilievska |
| 3.0 | 03.08.2019 | ISMS site | All Employees | Zhaneta Ilievska |
| 4.0 | 20.11.2019 | ISMS site | All Employees | Zhaneta Ilievska |
| 5.0 | 24.11.2020 | ISMS site | All Employees | Zhaneta Ilievska |
| 6.0 | 12.01.2021 | ISMS site | All Employees | Zhaneta Ilievska |
| 7.0 | 30.09.2021 | ISMS site | All Employees | Zhaneta Ilievska |
| 8.0 | 01.11.2021 | ISMS site | All Employees | Zhaneta Ilievska |
| 9.0 | 10.10.2022 | ISMS site | All Employees | Zhaneta Ilievska |
| 10.0 | 12.12.2022 | ISMS site | All Employees | Zlatko Chavdarovski |
| 11.0 | 02.01.2024 | ISMS Site | All Employees | Zlatko Chavdarovski |
| **12.0** | **25.12.2024** | **ISMS Site** | **All Employees** | Zlatko Chavdarovski |

**Document Sign-Off**

| Date | Signed-off By |
|---|---|
| | |



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

# 3 PURPOSE

This Policy provides guidance for using cryptography in INTERVORKS DOOEL branded as IWConnect (hereinafter the Company) to protect the confidentiality, authenticity or integrity of information. The algorithms used must have received substantial public review and have been proven to work effectively.

# 4 SCOPE

This policy applies to all employees, contractors, and third parties who access the company's resources and information systems, including those using the Company's devices and network infrastructure.

# 5 ENCRYPTION

The Company is using encryption to protect the information on workstations (laptops) and mobile devices and highly confidential information in transit or at rest.

## 5.1 Roles and responsibilities

The Information Security Manager (ISM) is responsible for formulating the cryptography rules, including determining which information and systems will be encrypted – where applicable, as well as choosing which encryption algorithms will be used. ISM is also responsible for periodical review and update of the rules and algorithms.

System Operations are responsible for the implementation of cryptographic rules and key/certificate management - generating, renewing, revoking and secure storage of keys/certificates.

## 5.2 Mobile Device Encryption

Most of the Company's employees use laptops as workstations. If these devices are stolen and their drives are not encrypted, the information will be readily available to unauthorized users. This is a vulnerability with unpredictable impact on the company's business. To prevent the risk and harden the attacker's efforts to access the information, these devices must be encrypted.

The encryption policy applies only to **laptops**.

If employees use smart phones to access, use and/or store company related business information from e-mails, Microsoft Teams or other company approved apps, they must do that by using *Microsoft Endpoint Manager* (*Intune*) enrolled device and separate work profile managed by the *Intune Company Portal* mobile application. These smart phone devices must be natively encrypted, and *Microsoft Endpoint Manager* actively monitors their encryption status with the possibility to retire (wipe out) the content from the work profile if required.

The operating systems used on most of the Company's laptops are Windows 10 and Windows 11. These operating systems have native support for BitLocker, which is using industry proven AES-128 or AES-256 encryption. Some portable devices use Linux, Android, MacOS or iOS and those portable devices must be encrypted as well.

Each laptop must have encrypted drives before it is used as an employee workstation. The encryption of the laptops is executed by *System Operations* only (device owners) and it is part of device preparation procedure before it is delegated to the employees (responsible for the particular device).

Each BitLocker encrypted device MAY have pre-boot PIN set if that laptop has TPM (Trusted Platform Module). Laptops without TPM MUST have a startup password set.

BitLocker generates Recovery Keys to access the information on the encrypted drives if they are removed from the laptop.



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

The Recovery Keys, pre-boot PINs and startup passwords MUST be kept secure and protected by *System Operations* only. The employees MUST not keep any Recovery Keys, pre-boot PINs and startup passwords on their laptops or elsewhere. Violating this rule is a very serious act against this policy.

The Company provides software development services and this kind of service requires daily activities like experimenting with various software like servers, development tools etc. To provide enough flexibility and support the business, each laptop user that is responsible for that device is a local Administrator too. The Administrator role on the local computer allows the employees to turn on/off drive encryption, re-print recovery keys etc. Doing this is **strongly prohibited** and it is a serious violation of this policy that administratively allows only *System Operations* to deal with drive encryption operations and recovery key maintenance.

Periodic inspections by *System Operations* and *Information Security Manager* must ensure that all company laptops have encrypted drives. Also, all Windows workstations are enrolled in Microsoft Intune and drive encryption is checked near real-time by Microsoft Endpoint Manager.

For external cooperators, the drive encryption policy applies only if they use company-owned laptops. If they are using personal devices, those devices must be enrolled in Intune, just like company-owned devices. However, the drives on personal devices will only be encrypted with the cooperator's permission. In this case, the cooperator is responsible for secure storage of the recovery key. In cases where personal devices used are not encrypted, the NDA documents signed with these third-party cooperators outline their responsibility for protecting Company owned information.

## 5.3 File Server Encryption

File servers that contain *Personally Identifiable Information* (e.g. employee or candidate CVs) have BitLocker encrypted drives. *System Operations* are responsible for the encryption process as well as the associated Recovery Keys.

## 5.4 Information Encryption

Per document Information Encryption is NOT mandatory in the Company.

When documents, code and other information are exchanged outside of the company (e-mail, VPN, remote code repository commit), the transport channel itself MUST be encrypted, i.e. TLS MUST be used for all incoming/outgoing connections (SMTP, IMAP, VPN).

Under some circumstances an employee may decide that some information is highly sensitive, and it must have encryption at rest or in transit. The encryption can be accomplished with **a 7-Zip envelope** that supports strong, password-based AES-256 encryption. The password for the envelope is exchanged through another communication channel like Skype or SMS.

The Company has local domain Certificate Authority. All domain users, through Active Directory Group policy, auto enroll for personal user and machine certificates, which have validity of 1 (one) year. The personal user certificates, if necessary, can be used for e-mail encryption.

The Company uses Exchange Online as an e-mail server. Employees can send some very sensitive confidential data encrypted with the **Microsoft Purview Message encryption** mechanism that does not require any cryptographic key distribution to the recipients. Recipients without Microsoft 365 account will be able to decrypt and see the message content with one-time passwords.

## 5.5 Encryption in Cloud Services

### 5.5.1 The Company as Customer

- **Cryptographic Controls Implementation** – The Company implements cryptographic controls for cloud services based on a thorough risk analysis. These controls must be robust

enough to mitigate identified risks, considering both our internal requirements and those provided by the cloud providers.

- **Evaluation of Provider Capabilities** – The Company will review the cryptographic capabilities offered by the cloud providers to ensure they meet the requirements set throughout this policy and are compatible with our existing cryptographic protections. This includes ensuring that cryptography is applied to data at rest and in transit.
- **Key Management** – Where applicable, the Company will identify and manage cryptographic keys for cloud services. If utilizing the key management services provided by the cloud providers, we will obtain detailed information about their key management procedures, including key lifecycle management (generation, storage, rotation, and destruction). The Company will not permit the cloud providers to manage our encryption keys if we employ our own key management system.
- **Protection of Personally Identifiable Information (PII)** – The Company acknowledges that certain jurisdictions may require the use of cryptography to protect specific types of PII. The Company will obtain information regarding the cloud provider's use of cryptography for PII protection and any capabilities available to assist us in implementing our own protections, including storage location of the PII.

### 5.5.2 The Company as a Provider

- **Use of Cryptography** – The Company will utilize cryptographic controls to protect data processed by our products hosted on cloud providers. This includes ensuring that our encryption measures comply with relevant standards and legal requirements.
- **Transparency and Customer Communication** – The Company will provide our customers with clear information about how we use cryptography to protect their data at rest and in transit. This includes outlining the circumstances under which encryption is applied and the measures in place to assist our customers in implementing additional protections.
- **Protection of Personally Identifiable Information (PII)** – The Company acknowledges that certain jurisdictions may require the use of cryptography to protect specific types of PII. The Company will provide our customers with clear information about the use of cryptography for PII protection, including storage location of the PII.

## 6 INTEGRITY – DIGITAL SIGNATURE

Per document Information Digital Signature is NOT mandatory in the Company.

Under some circumstances, especially e-mail information exchange, the sender may decide to digitally sign the message with his/her user certificate and provide message integrity proof that way. Note that the certificate used for digital signatures is issued by the local authority (Company CA) and these kinds of digital signatures do not provide global non-repudiation message integrity proof. However, it is enough to **ensure message integrity** for highly sensitive messages exchanged among employees and/or their clients.

It is also worth mentioning that Microsoft Purview Message Encryption encrypted e-mail messages implicitly verify the sender of the message.

## 7 LOCAL CERTIFICATE AUTHORITY

The Company maintains its local certificate authority (CA) integrated with Active Directory. This CA generates computer workstation, user and server RSA certificates. The key length for each certificate must be at least 2048 bits long. The workstation and user certificates are automatically renewed after their expiration. These certificates are used for:



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

- Workstation WLAN and LAN access (Computer certificate in conjunction with the RADIUS Network Policy Server for authentication and authorization)
- User WLAN and LAN access (User certificate in conjunction with the RADIUS Network Policy Server for authentication and authorization).
- E-Mail digital signature (User certificate)
- Web server TLS certificates

## 8 TRUSTED CERTIFICATE AUTHORITIES

Some of the Company's systems are configured with TLS certificates issued by trusted third party Certification Authorities. Same rules for key length and algorithms apply for generating certificates from trusted CAs as from the local CA.

## 9 TLS CRYPTOGRAPHY

All Company backbone systems must be exposed through *TLS* protocol. These internal systems MUST be configured with TLS certificates issued by the Company's local Certificate Authority. The TLS configuration MUST be configured with strong cipher suites that are a subset of the whole TLS 1.2 set of suites. All legacy encryption algorithms like *RC2* or *RC4* MUST NOT be used. All legacy hashing algorithms like *MD5* or *SHA-1* MUST NOT be used. The general guidelines when configuring *TLS* cipher suites on the servers are:

- Provide *Perfect Forward Secrecy*: Use *Elliptic Curve Diffie-Hellman Ephemeral* (ECDHE) key exchange
- Strong Symmetric Encryption Algorithm: Use *AES-256* or *AES-128* (the latest must be used with *Galois Counter Mode* (*GCM*) only)
- Encryption Mode: Using *Galois Counter Mode* (GCM) is preferable because the message blocks can be encrypted in parallel. This mode provides *integrity* on the encrypted data as well. The *Cipher Block Chaining* (*CBC*) mode can be used with *AES-256* only. This mode is not as secure as *GCM* because of the data stream block padding at the end (*GCM* does not use padding at all). The padding could be target of some known cipher attacks like the *Padding Oracle Attack*
- Strong *Message Authentication Code* (*MAC*) algorithms: Use *SHA-256* or *SHA-384*

The internal backbone servers and systems MUST be configured to accept the following *TLS* cipher suites at the specified order of preference:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The Company's public web site shall be configured with the same suites as well. Having this constrained set of strong cipher/suites may impact some older clients. This is an acceptable approach from a security perspective.

All web servers and their configured *TLS* should be monitored with Nagios. In particular, Nagios checks shall raise system alerts if:

- The web servers accept connections using any protocol below TLS 1.2 (SSLv3, TLS 1.1 etc.)



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

- The negotiated suite does not belong to the aforementioned. The web server must be configured properly in that case
- The server's certificate key length is less than 2048 bit long
- There are less than 14 days before the server's certificate expiration.

Note: The Company's Windows servers and workstations are regularly updated. Some of the updates are security updates. Up-to-date Windows system (server/workstation) will always have up-to-date TLS 1.2 cipher suites with correct suite preference order.

## 10 LINUX SERVER SSH CRYPTOGRAPHY

Linux servers MUST be accessed through strong SSH cipher suite and protocols.

The SSH protocol used must be SSH version 2. For newer systems version 1 is automatically disabled. For older systems, it must be explicitly configured in the SSH configuration file *sshd_config*:

```
Protocol 2
```

The host keys MUST obey the following key constraints:

- *RSA* key must be at least 2048 bits long (/etc/ssh/ssh_host_rsa_key)
- *ECDSA* key must be at least 256 bits long (/etc/ssh/ssh_host_ecdsa_key)
- ED25519 key must be at least 256 bits long (/etc/ssh/ssh_host_ed25519_key)

*DSA* (Digital Signature Algorithm) MUST be disabled in *sshd_config* (comment the HostKey entry).

The length of the host key can be determined with the following command:

```
sshkeygen -l -f <<key file>>
```

If the length does not obey the above rules, then SSH host key MUST be regenerated.

Symmetric algorithms for encrypting the bulk of transferred data are configured using the *Ciphers* option in the file *sshd_config*. Good algorithm values are:

- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

Host key algorithms are selected by the *HostKeyAlgorithms* option. Acceptable host key signature algorithms are:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-rsa

Key exchange algorithms are selected by the *KexAlgorithms* option. Acceptable algorithms are:

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

Message authentication code algorithms are configured using the *MAC* option. Acceptable algorithms are:

- hmac-sha2-256
- hmac-sha2-512

As a reference, the following article contains several SSH hardening related tips:

https://www.ssh.com/ssh/sshd_config/

# 11 VPN SERVER CRYPTOGRAPHY

To ensure the confidentiality of the data transmitted for client VPN and site-to-site VPN network communications the Company uses OpenVPN and IPsec VPN technology. Both VPN technologies are incorporated in the *pfSense* firewall and MUST be configured with strong cipher suites to ensure up to date and strong communication security.

## 11.1 IPsec site-to-site VPN Cryptography

IPsec VPN is used for site-to-site VPN connection among the Company's branch offices.

IPsec in both negotiation phases uses encryption algorithms, secure hash algorithms and public key cryptography protocols to establish a secure communication.

IKEv2 (*Key Exchange version*) MUST be used in Phase 1 in order to support the AES encryption algorithm with GCM (*Galois Counter Mode*) and 256 bit key size. The Hash algorithm must be set at least to SHA256, legacy algorithms like MD5 and SHA1 MUST not be used. DH (Diffie-Hellman) groups 1,2,22,23 and 24 provide weak security and MUST not be used, DH group 14 or higher (but not weak ones mentioned before) MUST be used.

Acceptable settings for *pfSense* Phase 1 are:

- Key Exchange version: IKEv2
- Encryption Algorithm: AES256-GCM with 128 bit ICV
- Hash Algorithms: SHA256 or higher
- PFS Group: 16

In Phase 2 same rules apply as in Phase 1, i.e. AES256-GCM encryption MUST be used with SHA256 or higher Hash Algorithm and Diffie-Hellman key exchange (PFS key group) with 2048 bit or longer modulus which corresponds to DH group 14 or higher (but not 22,23 and 24).

Acceptable settings for *pfSense* Phase 2 are:

- Protocol: ESP (Encapsulating Security Payload)
- Encryption Algorithms: AES256-GCM with 128 bit ICV
- Hash Algorithms: SHA256 or higher
- PFS key group 16 (4096 bit)

## 11.2 OpenVPN Client VPN Cryptography

OpenVPN technology is used for client VPN connections.

OpenVPN uses TLS for authentication, TLS1.2 version MUST be used with an RSA key at least 2048 bit long. DH parameter used for key exchange MUST be set to at least 2048 bit long modulus. Strong symmetric encryption algorithm with Galois Counter Mode (AES256-GCM) MUST be used. The hashing algorithm MUST be set to at least SHA256.

Acceptable settings for *pfSense* OpenVPN are:



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com

- RSA Key: 2048 bit long
- DH Parameter Length: 8192 bit
- Encryption Algorithm: AES256-GCM with 128 bit ICV
- Authentication digest algorithm: SHA256 or higher

## 12 LINUX PASSWORDS

Linux systems store the user passwords as salted hashes. The passwords MUST NOT be hashed using deprecated hash algorithms like *MD5*. The Company's Linux servers must encrypt user passwords using *SHA-512*.

For example, *Debian* based Linux systems keep the user passwords in the file */etc/shadow*. The first argument after the username is the hashing algorithm identifier. The identifier for *SHA-512* is **6**.

The password encryption method can be configured into the file */etc/login.defs*:

```
ENCRYPTION_METHOD SHA512
```

## 13 DEFINITIONS AND ABBREVIATIONS

| Term | Description |
|---|---|
| **Information** / data **in transit** | Information/data actively moving from one location to another such as across the internet or through a private network |
| Information at rest | Information/data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way |
| **Encryption** | Process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot |
| Digital signature | A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity) |
| Certificate authority (CA) | In cryptography, a **certificate authority** or **certification authority** (**CA**) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. |

## 14 RELATED DOCUMENTS

- *IW_Portable_Device_Policy*
- *IW_Secure_Acquisition_and_Development_Procedure*
- IW_Cloud Computing Policy



Office: Metodija Andonov - Chento 15, 7000 Bitola, Macedonia
phone: +389 (0) 47 221 914, fax: + 398 (0) 47 240 010
email: iwconnect@iwconnect.com