Załącznik nr 1 do instrukcji QI 21 20

Instrukcja dotycząca bezpieczeństwa informacji dla firm zewnętrznych

Information security procedures for external companies

Niniejsze wytyczne określają zasady bezpieczeństwa informacji, które muszą przestrzegać osoby trzecie podczas przebywania na terenie Spółek BURY, korzystania z informacji i urządzeń informatycznych (np. komputerów osobistych, stacji roboczych, smartfonów lub tabletów) na terenie Spółek BURY lub podczas podłączania się do systemów informatycznych Spółek BURY z zdalnych lokalizacji.

These guidelines define the rules of information security that must be followed by third parties while staying on the premises of the BURY Companies, using information and IT devices (e.g. personal computers, workstations, smartphones or tablets) on the premises of the BURY Companies or when connecting to the BURY IT systems from the remote locations.

Osoby trzecie zobowiązane są z zapoznaniem się i stosowaniem wymienionych zasad.

Third parties are required to read and apply the mentioned rules.

Osoby trzecie korzystające z dostępu zdalnego (pkt. 4) zobowiązane są do bezwzględnego stosowania zasad podanych w pkt. 3.

Third parties using remote access (point 4) are obliged to strictly apply the rules specified in point 3.

1. Podstawowe wymagania dla wszystkich osób trzecich / Basic requirements for all third parties

Wszystkie osoby trzecie, w tym pracownicy, wymienieni z imienia i nazwiska, muszą przejść szkolenie z zakresu Polityki Bezpieczeństwa Informacji, organizowane przez Spółkę BURY; szkolenie musi zostać potwierdzone na piśmie.

Zdarzenia związane z bezpieczeństwem informacji (np. podatności, naruszenia przepisów bezpieczeństwa informacji) dotyczące danych lub systemów Spółki BURY muszą zostać niezwłocznie zgłoszone do jednostki odpowiedzialnej (Dział zarządzania IT - DI).

Odkryte podatności lub słabe punkty dotyczące systemów IT Spółki BURY muszą być zgłaszane do jednostki odpowiedzialnej (Dział zarządzania IT - DI).

Każde podejrzenie utraty informacji należącej lub powiązanej z Spółką BURY musi być niezwłocznie zgłoszone do jednostki odpowiedzialnej (Dział zarządzania IT - DI).
Osoby współpracujące z Spółką BURY mogą otrzymać dedykowane nośniki identyfikujące (np. Karty Smartcard, SecureID) lub indywidualne kody dostępowe (loginy, hasła, profile połączeń VPN).

Karty dostępowe i dane logowania (loginy, hasła, tokeny) muszą zostać zwrócone do jednostki odpowiedzialnej (Dział zarządzania IT - DI) Spółki BURY w przypadku:

- zakończenia współpracy;
- braku konieczności korzystania z dostępów.

Korzystanie z danych dostępowych innych osób (karty dostępowe, loginy, tokeny) jest zabronione.
Przekazywanie danych dostępowych innym osobom (karty dostępowe, loginy, tokeny) jest zabronione.

Zapisywanie danych dostępowych (np., loginy, hasła, kody PIN) w postaci notatek, fiszek jest zabronione.

Pozostawienie niezabezpieczonego dostępu i odejściu od stanowiska jest zabronione. Należy stosować zabezpieczenia w postaci: wylogowania się, zablokowania ekranu chronionego hasłem.
Pobrane urządzenia należące do Spółki BURY należy zwrócić w przypadku zaprzestania korzystania z tych urządzeń lub w przypadku zakończenia współpracy lub zadania wymagającego tych urządzeń.

All third parties, including employees, mentioned by name and surname, must undergo training in the field of Information Security Policy, organized by the BURY Company; the training must be confirmed in writing.

Information security-related events (e.g. vulnerabilities, breaches of information security regulations) concerning the data or systems of the BURY Company must be immediately

reported to the responsible unit (IT Management Department - DI).

Discovered vulnerabilities or weaknesses regarding BURY's IT systems must be reported to the responsible unit (IT management department - DI).

Any suspicion of loss of information belonging to or related to the BURY Company must be immediately reported to the responsible unit (IT Management Department - DI).

Persons cooperating with the BURY Company may receive dedicated identification media (e.g. Smartcard, SecureID cards) or individual access codes (logins, passwords, VPN connection profiles).

Access cards and login data (logins, passwords, tokens) must be returned to the responsible unit (IT management department - DI) of the BURY Company in the case of:

- termination of cooperation;
- no access required.

Using other people's access data (access cards, logins, tokens) is prohibited.

It is forbidden to transfer access data to other people (access cards, logins, tokens).

It is forbidden to save access data (e.g. logins, passwords, PIN codes) in the form of notes, fiches.

Leaving unsecured access and departing from the position is prohibited. Use security measures in the form of: logging out, locking the password-protected screen.

Received devices belonging to the BURY company should be returned in the event of ceasing to use these devices or in the event of termination of cooperation or a task requiring these devices.

2. Dodatkowe wymagania dla osób trzecich przebywających na terenie Spółek / Additional requirements for third parties residing on the premises of the Companies

Poniższe wymagania muszą być spełnione przez osoby trzecie:

- oświadczenie zachowania poufności musi zostać podpisane podczas meldunku na recepcji Spółki BURY;
- przepisy dotyczące wnoszenia urządzeń informatycznych na teren Spółki lub do stref bezpieczeństwa muszą być przestrzegane;
- użycie oprogramowania lub sprzętu komputerowego należącego do trzeciej strony, nie zatwierdzonego przez Spółkę BURY jest zabronione;
- telefony, tablety, nośniki danych, nie wykorzystywane podczas pracy na terenie Spółki BURY muszą zostać zdeponowane na recepcji w depozycie;
- podłączanie sprzętu komputerowego lub sieciowego do sieci Spółki BURY bez szczegółowych uzgodnień z jednostką odpowiedzialną (Dział zarządzania IT - DI) jest

zabronione.

- wykorzystanie dostępu do Internetu dla celów prywatnych możliwe jest tylko w sieci WiFi BURY Guest i jest zabronione w innych sieciach mających dostęp do Internetu;
- poruszanie się po terenie Spółki BURY możliwe jest wyłącznie w asyście pracownika Spółki;
- osoby trzecie muszą posiadać przypiętą w widocznym miejscu plakietkę „gość";
- osoby trzecie mają dostęp do pomieszczeń w strefach pomarańczowych i czerwonych tylko pod specjalnym nadzorem;

The following requirements must be met by third parties:

- a declaration of confidentiality must be signed at the check-in at the reception of the BURY Company;
- regulations regarding bringing IT devices to the Company's premises or to security zones must be complied with;
- the use of software or hardware belonging to a third party, not approved by the BURY Company, is prohibited;
- telephones, tablets, data carriers, not used during work on the premises of the BURY Company, must be deposited at the reception desk;
- connecting computer or network equipment to the network of the BURY Company without detailed arrangements with the responsible entity (IT Management Department - DI) is prohibited;
- using the Internet access for private purposes is possible only in the BURY Guest WiFi network and is prohibited in other networks with Internet access;
- moving around the premises of the BURY Company is possible only with the assistance of an employee of the Company;
- third parties must have a „guest" badge pinned in a visible place;
- third parties have access to the rooms in the orange and red zones only under special supervision;

3. Dodatkowe wymagania dla osób trzecich mających dostęp do Systemów I Infrastruktury IT / Additional requirements for third parties with access to the IT Systems and Infrastructure

Poniższe wymagania muszą być spełnione przez osoby trzecie:

- umowa o zachowaniu poufności (NDA) musi zostać podpisana z stroną trzecią, przed przystąpieniem do pracy z systemami informatycznymi lub danymi Spółki BURY, zgodnie z obowiązującym standardem w Spółce BURY;
- tylko jednostki upoważnione (DI) mogą otwierać urządzenia informatyczne (zdjęcie pokrywy), dokonywać zmian w sprzęcie (np. instalacja/usuwanie dysków twardych i modułów pamięci, podłączanie urządzeń sieciowych) oraz dokonywać zmiany ustawień bezpieczeństwa (np. firewall, aktualizacje, działające usługi ustawienia przeglądarki);
- korzystanie z urządzeń informatycznych i danych Spółki BURY przez osoby trzecie wymaga wyraźnej zgody jednostki upoważnionej (DI). Spółka BURY ma prawo cofnąć wyrażoną zgodę w każdej chwili (zabronić dostępu/użytkowania) (np. w przypadku

nadużycia);

- użycie lub/i modyfikacja programów, konfiguracji serwerów, konfiguracji maszyn jest dozwolona tylko po uzyskaniu zgody jednostki upoważnionej (DI);
- każdy wykonawca, pracujący na udostępnionym przez Spółkę BURY wyposażeniu informatycznym (sprzęt oraz oprogramowanie) jest odpowiedzialny za zapewnienie właściwego wykorzystania informacji, programów i urządzeń informatycznych tylko do celów służbowych i w zakresie danego zlecenia ze strony Spółki BURY;
- wykorzystywanie udostępnionego przez Spółkę BURY wyposażenia informatycznego (sprzęt oraz oprogramowanie) do celów prywatnych jest zabronione;
- wykorzystywanie prywatnego oprogramowania i informacji na urządzeniach udostępnionych przez Spółkę BURY jest zabronione;
- wykorzystywanie nielicencjonowanego oprogramowania (pirackiego) jest zabronione; wykorzystywanie oprogramowania licencjonowanego na osobę trzecią możliwe jest tylko w zakresie obowiązywania licencji; strona trzecia ponosi odpowiedzialność za niewłaściwie użycie licencji;
- kopiowanie oprogramowania i danych należących do Spółki BURY na niezatwierdzone przez jednostkę upoważnioną (DI) nośniki danych jest zabronione;
- wykonywanie kopii zapasowych danych na których się pracuje dozwolone jest jedynie na zatwierdzone lokalizacje, podane przez jednostkę odpowiedzialną (Dział zarządzania IT - DI);
- kopie zapasowe muszą być traktowane także z odpowiednią ostrożnością, jak dane oryginalne;
- przekazywanie danych do innych osób trzecich bez pisemnej zgody ze strony Spółki BURY jest zabronione;
- podłączanie sprzętu komputerowego lub sieciowego osób trzecich do sieci Spółki BURY możliwe jest po wcześniejszym uzgodnieniu z jednostką odpowiedzialną (Dział zarządzania IT - DI); w takich przypadkach wymagane jest aby:
    a) sprzęt komputerowy posiadał zainstalowany i aktualny program antywirusowy, musi to zostać zweryfikowane i potwierdzone przez jednostkę odpowiedzialną (Dział zarządzania IT - DI);
    b) sprzęt komputerowy lub sieciowy został podłączony w obecności pracownika jednostki odpowiedzialnej (Dział zarządzania IT - DI);
    c) sprzęt komputerowy został przeskanowany pod kątem obecności malware przez pracownika jednostki odpowiedzialnej (Dział zarządzania IT - DI);
- podłączenie pamięci masowych i urządzeń posiadających pamięć masową (pendrive, karta pamięci, telefon, aparat) możliwe jest po wcześniejszym uzgodnieniu z jednostką odpowiedzialną (Dział zarządzania IT - DIWO); w takich przypadkach wymagane jest aby:
    a) pamięć masowa została przeskanowana pod kątem obecności malware przez pracownika jednostki odpowiedzialnej (Dział zarządzania IT - DI);
    b) podłączenie pamięci masowej do urządzeń Spółki BURY możliwe jest tylko w obecności pracownika jednostki odpowiedzialnej (Dział zarządzania IT - DI);
- w przypadku wygaśnięcia umowy pomiędzy Spółką BURY a osobą trzecią, wszystkie dane Spółki BURY muszą zostać zwrócone lub zniszczone. Protokół zniszczenia danych musi być niezwłocznie dostarczony do Spółki BURY.

The following requirements must be met by third parties:

- a confidentiality agreement (NDA) must be signed with a third party, prior to commencing work with IT systems or data of the BURY Company, in accordance with the applicable standard at the BURY Company;
- only authorized units (DI) can open IT devices (cover removal), make changes to hardware (e.g. install / remove hard drives and memory modules, connect network devices) and change security settings (e.g. firewall, updates, running services browser settings);
- the use of IT devices and data of the BURY Company by third parties requires the express consent of an authorized entity (DI). The BURY company has the right to withdraw the consent at any time (prohibit access / use) (e.g. in the event of abuse);
- the use and/or modification of programs, server configurations, machine configurations is allowed only after obtaining the consent of an authorized entity (DI);
- each contractor working on the IT equipment provided by the BURY Company (hardware and software) is responsible for ensuring the proper use of information, programs and IT devices only for business purposes and within the scope of a given order on the part of the BURY Company;
- the use of IT equipment (hardware and software) provided by the BURY Company for private purposes is prohibited;
- the use of private software and information on devices provided by the BURY Company is prohibited;
- the use of unlicensed (pirated) software is prohibited;
- third party licensed software may only be used within the scope of the license; the third party is responsible for the misuse of the license;
- copying the software and data belonging to the BURY Company onto data carriers not approved by the authorized entity (DI);
- backing up data on which you work is allowed only to approved locations, provided by the responsible unit (IT management department - DI);
- backups must also be treated with due care, as the original data;
- transferring data to other third parties without the written consent of the BURY Company is prohibited;
- connecting computer or network equipment of third parties to the network of the BURY Company is possible after prior arrangement with the responsible unit (IT Management Department - DI); in such cases, it is required that:
    a) the computer hardware has an installed and up-to-date antivirus program, this must be verified and confirmed by the responsible unit (IT management department - DI);
    b) the computer or network equipment was connected in the presence of an employee of the responsible unit (IT management department - DI);
    c) the computer hardware has been scanned for malware by an employee of the responsible unit (IT management department - DI);
- connection of mass storage devices and devices with mass memory (flash drive, memory card, telephone, camera) is possible after prior arrangement with the responsible unit (IT management department - DI); in such cases, it is required that:
    a) the mass memory was scanned for malware by an employee of the responsible entity (IT Management Department - DI);

b) connecting the mass memory storages to the devices of the BURY Company is possible only in the presence of an employee of the responsible unit (IT Management Department - DI);

- in the event of termination of the contract between the BURY Company and a third party, all data of the BURY Company must be returned or destroyed. The data destruction report must be immediately delivered to the BURY Company.

4. Dodatkowe wymagania dla osób trzecich korzystających z zdalnego dostępu / Additional Requirements for Third Party Remote Access Users

Zdalny dostęp identyfikowany jest przez:

- dostęp do infrastruktury IT zestawiany przez łączeinternetowe przy pomocy dedykowanych usług (np. VPN, Servery UAG, Wirtualne Systemy, Wirtualne Aplikacje);
- bezpośrednie połączenie z infrastrukturą Spółki BURY przy pomocy dedykowanych łączy;
- prace zdalne za pomocą połączeń wideokonferencji (np. Skype, Teams, Zoom);
  zdalny dostęp dozwolony jest na okres nie dłuższy niż 1 miesiąc, po tym czasie
- wszystkie dostępy są wyłączane i muszą być ponownie zweryfikowane;
- zdalny dostęp podlega logowaniu i monitoringowi;

Poniższe wymagania muszą być spełnione przez osoby trzecie:

- wymiana danych musi spełniać koncept bezpieczeństwa zgodny z procedurami Spółki BURY opisany w pkt 6;
- podczas połączeń wideokonferencyjnych osoby trzecie mają obowiązek upewnić się, że obraz lub dźwięk nie zostanie nagrany przez osoby postronne;
- podczas pracy zdalnej na zasobach Spółki osobytrzecie mają obowiązek wyłączenia/ wylogowania się z usług zewnętrznych (m.in. Google Drive, Dropbox)

Remote access is identified by:

- access to IT infrastructure compiled over the Internet using dedicated services (e.g. VPN, UAG Servers, Virtual Systems, Virtual Applications);
- direct connection with the infrastructure of the BURY company using dedicated links;
- remote work via videoconferencing (eg Skype, Teams, Zoom);
- remote access is allowed for a period not longer than 1 month, after that time all accesses are turned off and must be verified again;
- remote access is subject to logging and monitoring;

The following requirements must be met by third parties:

- data exchange must meet the security concept in accordance with the procedures of the BURY Company described in point 6;
- during videoconferencing, third parties are required to ensure that the image or sound is not recorded by third parties;
- when working remotely on the Company's resources, third parties are required to disable / log out of external services (including Google Drive, Dropbox).

5. Dodatkowe wymagania dla osób trzecich wdrażających lub serwisujących rozwiązania IT lub maszyny wspierane komputerowo / Additional requirements for third parties implementing or servicing IT solutions or computer-assisted machines

- Poniższe wymagania muszą być spełnione przez osoby trzecie:
  dokumentacja wdrożeniowa konfiguracji siecimusi zostać przedstawiona przed przystąpieniem do prac;
- konieczność bezpośredniego dostępu maszyny/systemu do Internetu musi zostać udokumentowana i podlega ciągłemu monitoringowi;
- połączenie systemu/maszyny z siecią Bury musi być wykonywane w obecności przedstawiciela jednostki odpowiedzialnej (Dział zarządzania IT - DIWO);
- wdrażany system/maszyna musi mieć możliwość nadzoru (monitoring);
  wdrażany system/maszyna musi posiadać udokumentowaną procedurę zatrzymywania i uruchamiania, kopii zapasowej oraz odtworzenia;
- wdrażany system/maszyna musi mieć możliwość:
  a) zmiany haseł, hasła nie mogą być hardkodowane (‘hardcoded’)
  b) aktywowania i dezaktywacji użytkowników;
  c) oddzielenia użytkowników operacyjnych od administratorów systemu/maszyny;
- wdrażany system/maszyna musi posiadać ochronę antywirusową (o ile ma zastosowanie);
- wdrażany system/maszyna będzie podlegaćregularnym skanom podatności, wdrożenie systemu bez aktualnych zabezpieczeń lub z krytycznymi podatnościami jest niedozwolone;

The following requirements must be met by third parties:

- implementation documentation of the network configuration must be submitted prior to the commencement of works;
- the need for direct access of the machine / system to the Internet must be documented and is subject to constant monitoring;
- the connection of the system / machine to the Bury network must be made in the presence of a representative of the responsible entity (IT management department - DIWO);
- the implemented system / machine must be able to be supervised (monitoring);
  the system / machine being implemented must have a documented stop and start, backup and recovery procedure;
- the implemented system / machine must be able to:
  a) changing passwords, passwords cannot be ‚hardcoded’
  b) user activation and deactivation;
  c) separation of operational users from system / machine administrators;
- the implemented system / machine must have anti-virus protection (if applicable);
- the implemented system / machine will be subject to regular vulnerability scans, implementation of the system without up-to-date security or with critical vulnerabilities is not allowed;

6. Komunikacja i wymiana informacji / Communication and information exchange

Komunikacja i wymiana informacji możliwa jest przez dowolną metodę przekazywania danych na odległość, tj:

- fax;
- rozmowa telefoniczna;
- wideokonferencja;
- wiadomość email.

Podczas wymiany danych poufnych lub tajnych strona trzecia zobowiązana jest do:

- korzystania tylko z oficjalnych adresów email, numerów faksu, numerów telefonów podanych lub potwierdzonych przez pracownika Spółki BURY, lub dostępnych na stronie bury.com;
- nie umieszczania danych tajnych lub poufnych w wiadomościach email bez wcześniejszego zaszyfrowania tych danych; szyfrowanie danych musi być wykonane algorytmem AES-256;
- hasło do zaszyfrowanych plików musi zostać przekazane innym kanałem komunikacyjnym (np. rozmowa telefoniczna, pocztą w zapieczętowanej kopercie);
- korzystania z bezpiecznego systemu wymiany danych wspierającego szyfrowanie w transporcie, możliwe jest wykorzystanie systemu Spółki BURY (Fileshare);

Communication and information exchange is possible by any method of remote data transmission, i.e.:

- fax;
- call;
- videoconference;
- email message.

When exchanging confidential or secret data, the third party is obliged to:

- use only official e-mail addresses, fax numbers, telephone numbers provided or confirmed by an employee of the BURY Company, or available at bury.com;
- not placing secret or confidential data in e-mail messages without first encrypting the data; data encryption must be performed with the AES-256 algorithm;
- the password for encrypted files must be transferredto another communication channel (e.g. phone call, by mail in a sealed envelope);
- using a secure data exchange system supporting encryption in transport, it is possible to use the BURY (Fileshare) company system;

Skróty stosowane w Instrukcji / Abbreviations used in the Manual:

DI	-	**Dział Zarządzania IT**	-	IT Management Department
osoba trzecie / third party	-	osoba fizyczna, przedsiębiorca lub jednostka prawna, która świadczy usługi na rzecz Spółek BURY	-	a natural person, entrepreneur or legal entity who provides services to the BURY Companies
wykonawca	-	patrz „osoba trzecia”	-	see “third party”
dostawca	-	patrz „osoba trzecia”	-	see “third party”
zamawiający	-	Spółka BURY	-	Bury company