**WYPOSAŻENIE POMIESZCZEŃ**

**I PIĘTRO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| POMIESZCZENIE 19. PRACOWNIA PLASTYCZNA | | | | | |
| Nr | Opis | Źródło | Rysunek | Ilość |
| 1 | Suszarka podwójna na prace plastyczne - 50 prac | Metalowa suszarka do prac plastycznych. Wyposażona w kółeczka i możliwość regulacji. Stelaż suszarki pokryty lakierem epoksydowym. Suszarka posiada z dwóch stron po 25 poziomów do ułożenia prac.  Wym.: ok.65 x 41 x 97 cm | https://www.educol.pl/24346-large_default/suszarka-podwojna-na-prace-plastyczne-50-prac.jpg | 1 |
| 2 | Regulowany stół kreślarski | Regulowane biurko  -Możliwość regulacji wysokości (od 65 do 90.5 cm) oraz zmiany kąta nachylenia blatu  -2 blaty robocze (jeden ze zmianą kąta nachylenia, drugi płaski) umożliwiają pracę przy wielu zadaniach jednocześnie  -2 szuflady znajdujące się pod blatem zapewniają dodatkową przestrzeń do przechowywania  - organizer po prawej stronie na ołówki, długopisy oraz inne akcesoria  -taboret wyściełany grubą warstwą gąbki  - konstrukcja z wysokiej jakości wodoodpornej płyty MDF oraz wytrzymałego metalu  -4 duże antypoślizgowe podkładki  Materiał MDF,PVC,metal  Szerokość (cm)115  Długość (cm)61,5  Wysokość (cm)65-90,5  Waga (kg) 26 | Regulowany stół kreślarski | 20 |
| 3 | Szafka Na Rysunki | Specyfikacja produktu  Wysokość:1135 mm  Szerokość:990 mm  Głębokość:680 mm  Format:A1  Materiał:Laminat  Kolor górnej płyty:Buk  Ilość szuflad:15  Nośność szuflady:15 kg  Szyny szuflady:Szyna ślizgowa | https://wyposazamyfirmy.pl/images/artykuly/1/AJ_105431.jpg | 3 |
| 4 | Regały  (zabudowa) z półkami otwartymi i zamkniętymi. | Przesuwne drzwi.  Wymiary:  Wysokość: dopasowana do wysokości pomieszczenia  Głębokość: 60 cm  Długość: 4 m |  | 1 |
| 5 | Myjnia wykona ze stali nierdzewnej z dwoma stanowiskami | Wymiary:  Długość umywalki: 1m  Liczba stanowisk: 2  Typ: rynnowa  Materiał: stal nierdzewna | Umywalki chirurgiczne | 1 |
| 6 | Laptop | Komputer Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.  Ekran Matryca TFT, 15,6” z podświetleniem w technologii LED matowa lub z powłoką antyrefleksyjną, rozdzielczość: FHD 1920x1080  Obudowa Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.140 stopni.  Chipset Dostosowany do zaoferowanego procesora  Płyta główna Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s).  Wydajność Model procesora: Osiągający wynik minimum 7 000 pkt w teście Passmark CPU Benchmarks według wyników ze strony www.cpubenchmark.net, zawartych w Załączniku Nr 1.2.a do SWZ (wyniki pochodzą z dnia publikacji postępowania). Informacje o oferowanym procesorze Wykonawca wskazuje w Formularzu cenowym.  Pamięć operacyjna Min. 16GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 2666MHz.  Dysk twardy Min. 240GB SSD zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.  Karta graficzna Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie  Audio/Video Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1,5W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), wbudowana kamera HD720p  Karta sieciowa Zintegrowana z płytą główną 10/100/1000 – RJ 45  Porty/złącza 2xUSB 3.1, 1x USB 3.1 typ-C, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC).  Klawiatura Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym.  WiFi Wbudowana karta sieciowa, pracująca w standardzie AC  Bluetooth Wbudowany moduł Bluetooth 4.2  Bateria Bateria – min. 3 komorowa 3500mAh, pozwalająca na nieprzerwaną pracę urządzenia do 6 godzin.  Zasilacz Zasilacz zewnętrzny max 65W  BIOS BIOS zgodny ze specyfikacją UEFI.  Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:  - wersji BIOS  - nr seryjnym komputera  - ilości pamięci RAM  - typie procesora i jego prędkości  -modele zainstalowanych dysków twardych  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynnośći: Możliwość ustawienia hasła dla twardego dysku  Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password  Możliwość ustawienia hasła Administratora i użytkowanika BIOS Mozliwość włączania/wyłaczania wirutalizacji z poziomu BIOSU  Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Bezpieczeństwo - złącze Kensington Lock,  - Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego (TPM 2.0).  Waga/Wymiary Waga urządzenia z baterią podstawową maksymalnie 2,2kg  Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty trzeba podać nazwę oferowanego oprogramowania System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB+++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:  • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,  • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,  • stosowanie kwarantanny,  • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)  • skanowanie urządzeń USB natychmiast po podłączeniu,  • automatyczne odłączanie zainfekowanej końcówki od sieci,  • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.  • Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.  • Musi posiadać moduł ochrony IDS/IPS  • Musi posiadać mechanizm wykrywania skanowania portów  • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów  • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją  tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do  200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64- bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Gwarancja  czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować  przez cały okres dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) |  |  |
| 7 | PROJEKTOR Z RZUTNIKIEM  Rozwijany elektrycznie  Wymiary ekranu200 x 200 cm  Format16:9  Przekątna obrazu 86 [cale]  Czarne ramki boczne5 cm  Wymiary obrazu190 x 107 cm  Czarny TOP89 cm  Czarny dół 4 cm  Przekrój kasety6.7 x 7.5 cm  Materiał obudowy stal  Rodzaj powierzchni Matt White  Rodzaj sterowania ścienne + bezprzewodowe  Rodzaj silnika tubowy |  |  | 1 |
| 8 | Dwudrożna kolumna aktywna 170w | Specyfikacja:  Głośnik wysokotonowy: 1” tytanowa membrana, 8 Ohm  Głośnik niskotonowy: 10”, 30 oz, 1,5” cewka  Pasmo przenoszenia: 30Hz – 20KHz  Czułość: 93dB +/- 2dB  Impedancja: 4 Ohm  Wartość SPL: 91dB  Funkcje: Reverb, Bluetooth  Wejścia mikrofonowe: XLR i Jack  Wejścia liniowe: Phono i AUX  Wyjście: XLR  Regulacja: Głośność (Mic, Reverb, Line, Master), Treble, Bass, Bluetooth on/off  Opcje mocowania: Stopki na spodzie odbudowy, standardowe wejście 35mm na statyw lub punkt mocujący 8mm  Materiał obudowy: Plastik  Waga: 7,2kg  Wymiary: 49 x 31 x 25cm | https://supersound.pl/media/catalog/product/cache/1/image/17f82f742ffe127f42dca9de82fb58b1/p/o/pol_pl_stagg-pms-10-eu-dwudrozna-kolumna-aktywna-170w-5357_1.jpg | 1 |
| 9 | Rolety zaciemniające | Roleta dzień noc na wymiar |  | 13 |
| 10 | Studyjna Lampa z klipsem i statywem | Charakterystyka:  lampa 15W (ekwiwalent 100W) energooszczędna żarówka w technologii Daylight (6000K)  CRI: 80+  Rzeczywiste eksponowanie kolorów bez przekłamywania ich tonacji.  Nowe szerszy klosz rozpraszający światło na większy obszar pracy. Kolor: oksydowany chrom  Stabilny, solidny trójnożny statyw o wysokości 2,2m mieszczący do 4 lamp w kolorze czarnym  Praktyczny, łatwo dostępny włącznik na szczycie klosza  Szybki i stabilny system mocowania blokowanym klipsem  Możliwość podłączenia dodatkowych lamp (do 4 na statywie) | https://warsztatartysty.pl/img/9609/studyjna-lampa-z-klipsem-i-statywem-32w | 4 |
| 11 | Sztaluga plenerowa | Waga: 3,3 kg,  wykonana z wysokiej jakości impregnowanego drewna bukowego  Regulowane nogi oraz szeroki kąt nachylenia. Nogi zakończone antypoślizgową gumą,  Półka oraz uchwyt trzymający podobrazie, regulowane za pomocą motylkowych nakrętek.  składana  Maksymalna wysokość podobrazia: 102 cm  Dopuszczalne obciążenie to max. 4 kg  Wymiary po złożeniu: 85 x 35 x 12 cm  Wymiary po rozłożeniu: 200 x 70 cm  Sztaluga do użytku zewnętrznego jak i wewnętrznego. |  | 20 |
| 12 | Krzesło sztaplowane | Konstrukcja  - kubełkowe siedzisko odlane z jednego kawałka czarnego polipropylenu  - wytrzymała konstrukcja ze stali  - siedzisko i oparcie wykonane z wysokogatunkowego tworzywa jest stabilne i wytrzymałe na obciążenie do 120 kg  Funkcjonalność:  -całkowicie odporne na wchłanianie substancji brudzących  - nogi krzesła zakończone stopkami z tworzywa sztucznego  - waga 2,6 kg  - sztaplowane do 12 sztuk. | https://krzeslabankietowe.pl/842-large_default/maxi-cr-czarna.jpg | 20 |
| 13 | ŚMIETNIKI DO SEGREGACJI  • 3 komory każda o pojemności 9l  • trzy kolory pokryw: beżowy, kremowy, brązowy  • pokrywy typu „klik” |  |  | 1 |